



OfficeConnect® Cable/DSL Router User Guide

3CR858-91

<http://www.3com.com/>

Part No. DUA8589-1AAA01

Rev. 01

Published July 2004



3Com Corporation
350 Campus Drive,
Marlborough, MA
USA 01752-3064

Copyright © 2004, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, and the 3Com logo are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

Wi-Fi and the Wi-Fi logo are registered trademarks of the Wi-Fi Alliance.

IEEE and 802 are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

ABOUT THIS GUIDE

- Naming Convention 7
- Conventions 8
 - Feedback about this User Guide 8
 - Related Documentation 9

1 INTRODUCING THE ROUTER

- OfficeConnect Cable/DSL Router 11
- Router Advantages 13
- Package Contents 13
- Minimum System and Component Requirements 14
- Front Panel 14
- Rear Panel 16

2 HARDWARE INSTALLATION

- Introduction 17
 - Safety Information 17
- Positioning the Router 17
 - Using the Rubber Feet 18
- Wall Mounting 18
- Connecting the Router 18

3 SETTING UP YOUR COMPUTERS

- Obtaining an IP Address Automatically 21
 - Windows 2000 21
 - Windows XP 23
 - Windows 95/98/ME 23
 - Macintosh 23
- Disabling PPPoE and PPTP Client Software 24

Disabling Web Proxy 24

4 RUNNING THE SETUP WIZARD

Accessing the Wizard 25

- Password 27
- Time Zone 28
- Connection Type 29
- DNS 35
- Hostname and MAC Address 36
- LAN Settings 37
- Configuration Summary 38

5 ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages 39

- Main Menu 39
- LAN Settings 40
- Internet Settings 42
 - Connection to ISP 43
 - DNS 49
 - Hostname & MAC 50
- Firewall 50
 - SPI 51
 - Special Applications 54
 - Virtual Servers 56
 - Client IP Filters 57
 - MAC Address Filtering 62
 - DMZ 63
- VPN 64
 - Adding an IPSec Connection 67
 - Adding an L2TP over IPSec Connection 68
 - Adding a PPTP Connection 70
- SNMP 71
- System Tools 72
 - Restart Router 73
 - Reset to Factory Defaults 73
 - Backup/Restore Settings 74
 - Upgrade 75

Admin Password	76
Time Zone	77
Advanced	79
NAT	79
Universal Plug and Play	80
WAN Ping Blocking	81
Remote Administration	81
Routing	82
DDNS	86
Status and Logs	87
Status	87
Traffic Metering	88
Logs	88
Support/Feedback	89
Support	89
Feedback	90

6 TROUBLESHOOTING

Basic Connection Checks	91
Browsing to the Router Configuration Screens	91
Connecting to the Internet	92
Forgotten Password and Reset to Factory Defaults	93
Alert LED	93
Power LED or Power Adapter OK LED Not Lit	94
Replacement Power Adapters	94
Recovering from Corrupted Software	95
Frequently Asked Questions	96

A IP ADDRESSING

The Internet Protocol Suite	99
Managing the Router over the Network	99
IP Addresses and Subnet Masks	99
How does a Device Obtain an IP Address and Subnet Mask?	101
DHCP Addressing	101
Static Addressing	101
Auto-IP Addressing	101

B ISP INFORMATION

C TECHNICAL SPECIFICATIONS

OfficeConnect Cable/DSL Router 105
Standards 105

D SAFETY INFORMATION

E OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product to Gain Service Benefits 111
Purchase Value-Added Services 111
Troubleshoot Online 111
Access Software Downloads 112
Contact Us 112
Telephone Technical Support and Repair 112

F END USER SOFTWARE LICENSE AGREEMENT

GLOSSARY

REGULATORY NOTICES

INDEX

ABOUT THIS GUIDE

This guide describes how to install and configure the OfficeConnect Cable/DSL Router (3CR858-91).

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Routers.



If a release note is shipped with the Cable/DSL Router and contains information that differs from the information in this guide, follow the information in the release note.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

<http://www.3com.com>

Naming Convention

Throughout this guide, the OfficeConnect Cable/DSL Router is referred to as the "Router".

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.

Conventions

[Table 1](#) and [Table 2](#) list conventions that are used throughout this guide.

Table 1 Notice Icons




Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 Text Conventions

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"> ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- OfficeConnect Cable/DSL Router User Guide
- Part Number DUA8589-1AAA01
- Page 24



Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to [Appendix E "Obtaining Support for your Product"](#).

Related Documentation

In addition to this guide, each Router document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Router.

1

INTRODUCING THE ROUTER

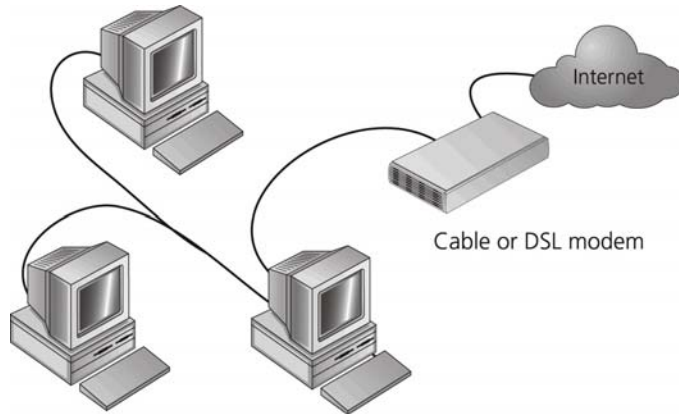
Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage.

OfficeConnect Cable/DSL Router

The OfficeConnect Cable/DSL Router is designed to provide a cost-effective means of sharing a single broadband Internet connection amongst several computers. The Router also includes an electronic “firewall” that protects your network using Stateful Packet Inspection (SPI) to detect intruders and prevent them from seeing your files or damaging your computers. The Router can also prevent your users from accessing Web sites which you find unsuitable. This completely equipped, Cable/DSL Router also features Virtual Private Network (VPN) initiation and termination, allowing encrypted links to other private networks.

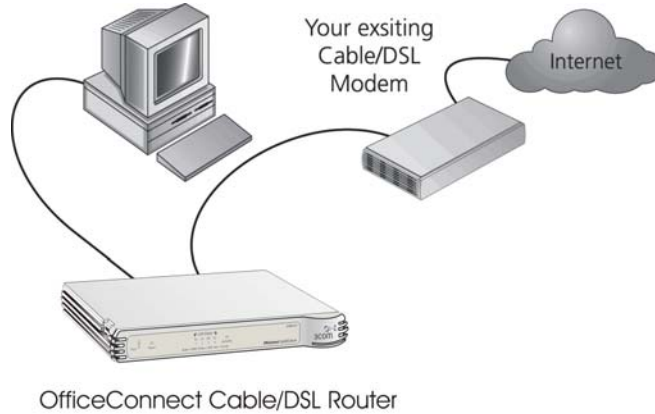
The example in [Figure 1](#) shows a network without a Router where only one computer is connected to the Internet. This computer must always be powered on for the other computers on the network to access the Internet.

Figure 1 Example Network Without a Router



When you use the Router in your network ([Figure 2](#)), it becomes your connection to the Internet. Connections can be made directly to the Router, or to an OfficeConnect Switch or Hub, expanding the number of computers you can have in your network.

Figure 2 Example Network Using a Cable/DSL Router



Router Advantages

The advantages of the Router include:

- Shared Internet connection for wired computers. The Cable/DSL Router also provides shared internet connection
- No need for a dedicated, “always on” computer serving as your Internet connection
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers
- Easy-to-use, Web-based setup and configuration
- Provides centralization of all network address settings (DHCP)
- Acts as a Virtual server to enable remote access to Web, FTP, and other services on your network
- Security - Firewall protection against Internet hacker attacks and encryption to protect network traffic

Package Contents

The Router kit includes the following items:

- One OfficeConnect Cable/DSL Router
- One power adapter for use with the Router
- Four rubber feet
- One Ethernet cable
- One CD-ROM containing the Router Discovery program and this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer

If any of these items are missing or damaged, please contact your retailer.

Minimum System and Component Requirements

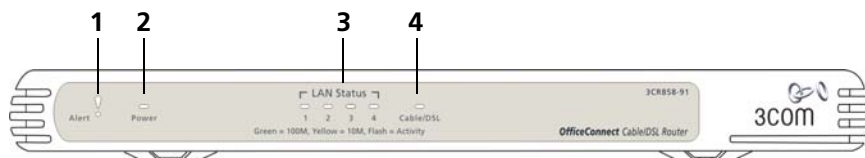
Your Router requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Router.
- A cable or DSL broadband connection to the Internet, with a suitable modem. The modem must have an Ethernet port for connection to your Router.
- A Web browser that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

Front Panel

The front panel of the Router contains a series of indicator lights (LEDs) that help describe the state of various networking and connection operations.

Figure 3 Router - Front Panel



1 Alert LED

Orange

Indicates a number of different conditions, as described below.

Off - The Router is operating normally.

Flashing quickly - Indicates one of the following conditions:

- The Router has just been started up and is running a self-test routine, or
- The administrator has invoked the *Reset to Factory Defaults* command, or
- The system software is in the process of being upgraded

In each of these cases, wait until the Router has completed the current operation and the alert LED is Off.

Flashing slowly - The Router has completed the *Reset to Factory Defaults* process, and is waiting for you to reset the unit. To do this, remove power, wait 10 seconds and then re-apply power. The Router will then enter the start-up sequence and resume normal operation.



If you have used a cable to reset the unit to Factory Defaults, refer to [“Forgotten Password and Reset to Factory Defaults”](#) on [page 93](#).

On for 2 seconds, and then off - The Router has detected and prevented a hacker from attacking your network from the Internet.

Continuously on - A fault has been detected with your Router during the start-up process. Refer to [Chapter 6 “Troubleshooting”](#).

2 Power LED

Green

Indicates that the Router is powered on.

3 Four LAN Status LEDs

Green (100Mbps link) / yellow (10Mbps link)

If the LED is on, the link between the port and the next piece of network equipment is OK. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, nothing is connected, the connected device is switched off, or there is a problem with the connection (refer to [Chapter 6 “Troubleshooting”](#)). The port will automatically adjust to the correct speed and duplex.

4 Cable/DSL Status LED

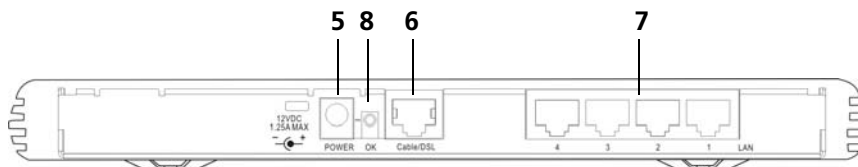
Green (100Mbps link) / yellow (10Mbps link)

If the LED is on, the link between the Router and the cable or DSL modem is OK. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, nothing is connected, the modem is switched off or there is a problem (refer to [Chapter 6 “Troubleshooting”](#)).

Rear Panel

The rear panel (Figure 4) of the Router contains four LAN ports, one Ethernet Cabler/DSL port, and a power adapter socket.

Figure 4 Router - Rear Panel



5 Power Adapter Socket

Only use the power adapter supplied with this Router. Do not use any other adapter.

6 Ethernet Cable/DSL port

Use the supplied patch cable to connect the Router to the Ethernet port on your cable or DSL modem. The port will automatically adjust to the correct speed and duplex.

7 Four 10/100 LAN ports

Using suitable RJ-45 cable, you can connect your Router to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). The LAN ports are configured as MDIX, for connection to a computer with a straight through RJ-45 cable.

8 Power Adapter OK LED

Green

Indicates that the power adapter is supplying power to the Router. If the LED is off, there may be a problem with the power adapter or adapter cable.

2

HARDWARE INSTALLATION

Introduction

This chapter will guide you through a basic installation of the Router, including:

- [“Positioning the Router”](#).
- [“Connecting the Router”](#).

Safety Information



WARNING: Please read the [“Safety Information”](#) section in [Appendix D](#) before you start.



VORSICHT: Bitte lesen Sie den Abschnitt [“Wichtige Sicherheitshinweise”](#) sorgfältig durch, bevor Sie das Gerät einschalten.



AVERTISSEMENT: Veuillez lire attentivement la section [“Consignes importantes de sécurité”](#) avant de mettre en route.

Positioning the Router

You should place the Router in a location that:

- is conveniently located for connection to the telephone socket.
- allows convenient connection to the computers that will be connected to the four LAN ports on the rear panel, if desired.
- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.

When positioning your Router, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.

- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. 3Com recommends you provide a minimum of 25 mm (1 in.) clearance.

Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Router from moving around on your desk or when stacking with flat top units. Only stick the feet to the marked areas at each corner of the underside of your Router.

Wall Mounting

There are two slots on the underside of the Router that can be used for wall mounting.



When wall mounting the unit, ensure that it is within reach of the power outlet.

You will need two suitable screws to wall mount the unit. To do this:

- 1 Ensure that the wall you use is smooth, flat, dry and sturdy and make two screw holes which are 150 mm (5.9 in.) apart.
- 2 Fix the screws into the wall, leaving their heads 3 mm (0.12 in.) clear of the wall surface.
- 3 Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.



When making connections, be careful not to push the unit up and off the wall.



CAUTION: *Only wall mount single units, do not wall mount stacked units.*

Connecting the Router

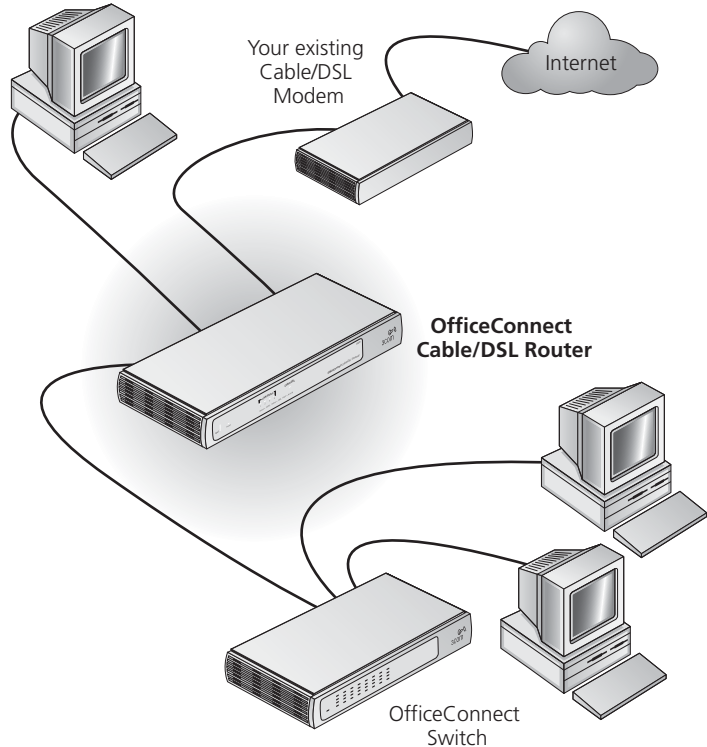
To power up your Router, and then connect it to your modem and to a computer, do the following:

- 1 Plug the power adapter into the power adapter socket located on the back panel of the Router.
- 2 Plug the power adapter into a standard electrical wall socket. Wait for the Alert LED to stop flashing.

- 3 Ensure that your modem and computer are both switched on.
- 4 Use the supplied cable to connect the Router's Ethernet Cable/DSL port to the modem. Check that the Cable/DSL Status LED lights.
- 5 Connect your computer to one of the 10/100 LAN ports on the Router. Check that the LAN Status LED for the port lights green.

See [Figure 5](#) for an example configuration.

Figure 5 Connecting the Router



3

SETTING UP YOUR COMPUTERS

The Router has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

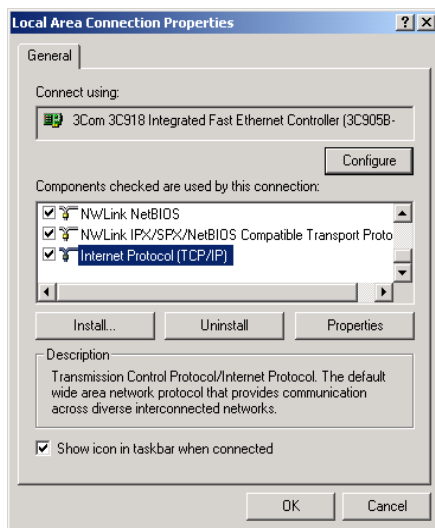
Obtaining an IP Address Automatically

Follow the instructions for your particular operating system to ensure that your computers are configured to obtain an IP address automatically.

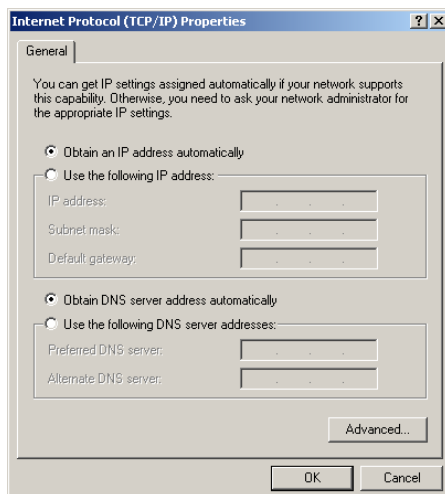
Windows 2000

If you are using a Windows 2000-based computer, use the following procedure to change your TCP/IP settings:

- 1 From the Windows *Start* Menu, select *Settings > Control Panel*.
- 2 Double click on *Network and Dial-Up Connections*.
- 3 Double click on *Local Area Connection*.
- 4 Click on *Properties*.
- 5 A screen similar to [Figure 6](#) should be displayed. Select *Internet Protocol TCP/IP* and click on *Properties*.

Figure 6 Local Area Properties Screen

- 6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS server address automatically* are both selected as shown in [Figure 7](#). Click **OK**.

Figure 7 Internet Protocol (TCP/IP) Properties Screen

- 7 Restart your computer.

Windows XP If you are using a Windows XP computer, use the following procedure to change your TCP/IP settings:

- 1 From the Windows *Start* menu, select *Control Panel*.
- 2 Click on *Network and Internet Connections*.
- 3 Click on the *Network Connections* icon.
- 4 Double click on *LAN or High Speed Connection* icon. A screen titled *Local Area Connection Status* will appear.
- 5 Select *Internet Protocol TCP/IP* and click on *Properties*.
- 6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS servers automatically* are both selected. Click *OK*.
- 7 Restart your computer.

Windows 95/98/ME If you are using a Windows 95/98/ME computer, use the following procedure to change your TCP/IP settings:

- 1 From the Windows *Start Menu*, select *Settings > Control Panel*.
- 2 Double click on *Network*. Select the *TCP/IP* item for your network card and click on *Properties*.
- 3 In the TCP/IP dialog, select the *IP Address* tab, and ensure that *Obtain IP address automatically* is selected. Click *OK*.

Macintosh If you are using a Macintosh computer, use the following procedure to change your TCP/IP settings:

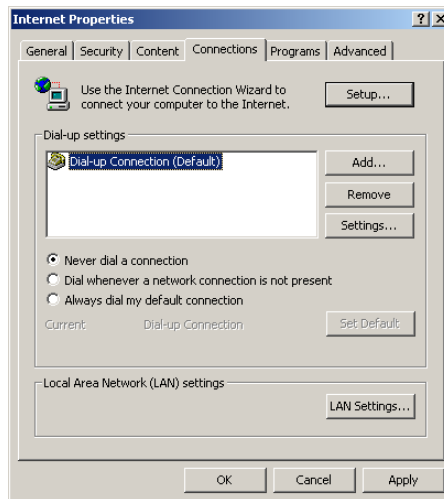
- 1 From the desktop, select *Apple Menu*, *Control Panels*, and *TCP/IP*.
- 2 In the *TCP/IP* control panel, set *Connect Via:* to "Ethernet".
- 3 In the *TCP/IP* control panel, set *Configure:* to "Using DHCP Server."
- 4 Close the *TCP/IP* dialog box, and save your changes.
- 5 Restart your computer.

Disabling PPPoE and PPTP Client Software

If you have PPPoE client software installed on your computer, you will need to disable it. To do this:

- 1 From the Windows *Start* menu, select *Settings > Control Panel*.
- 2 Double click on *Internet Options*.
- 3 Select the *Connections* Tab. A screen similar to [Figure 8](#) should be displayed.
- 4 Select the *Never Dial a Connection* option.

Figure 8 Internet Properties Screen



You may wish to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Router.

Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click *LAN Settings* at the bottom. Make sure that the *Use Proxy Server* option is unchecked.

4

RUNNING THE SETUP WIZARD

Accessing the Wizard

The Router setup program is Web-based, which means that it is accessed through your Web browser (Netscape Navigator or Internet Explorer).

To use the Setup Wizard:

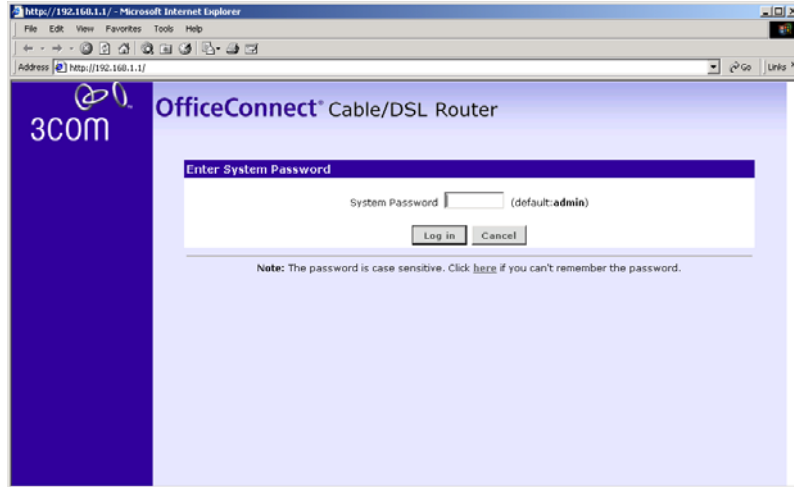
- 1 Ensure that you have at least one computer connected to the Router. Refer to [Chapter 2](#) for details on how to do this.
- 2 Launch your Web browser on the computer.
- 3 Enter the following URL in the location or address field of your browser: **http://192.168.1.1** (as shown in [Figure 9](#)).

Figure 9 Web Browser Location Field (Factory Default)



The Login screen displays (Figure 10).

Figure 10 Router Login Screen



- 4 Log in by typing the administrator password (the default password is **admin**) in the *System Password* field, and clicking *Log in*.



Be sure to bookmark this screen for easy reference if you should want to change the Router settings.


The Wizard will attempt to launch automatically, but if it fails, select Setup Wizard from the main menu.


- 5 You will be guided step by step through a basic setup procedure, described in the following sections. At any time, click *Next* to move to the next screen, click *Back* to return to the previous screen, or click *Cancel* to exit the Wizard.

Password Figure 11 Admin Password Screen

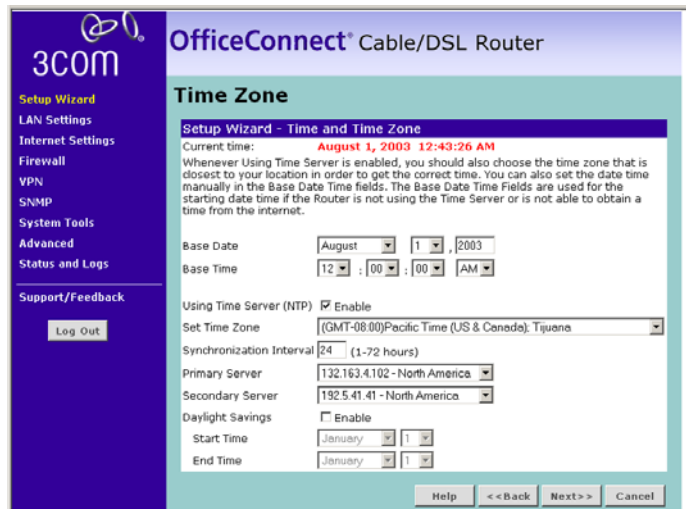
In the *Admin Password* screen ([Figure 11](#))

- 1 Type the *Current Password*.
- 2 Type a new password in both the *New Password* and *Confirm New Password* boxes.
- 3 Type in a *Login Timeout*. This is the amount of time you want the Router to remain inactive before it returns to the login screen.

 *3Com recommends entering a new password when setting up the Router for the first time. The Router is shipped from the factory with a default password, **admin**.*

 *The Password is case sensitive. Write the new password down and keep it in a safe place, so that you can change your settings in the future.*

- 4 Click *Next* to display the *Time Zone* setup screen ([Figure 12](#)).

Time Zone Figure 12 Time Zone Screen

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the Internet. The synchronized clock in the Router is used to record the security log. To set the time zone for your Router, do the following:

- 1 Select the *Base Date* and *Base Time*. The Router will use these settings if it is unable to connect to the Internet or SNTP Server.
- 2 To enable SNTP, check the *Using Time Server (NTP)* check box.
- 3 Select a time zone from the *Set Time Zone* drop down list.
- 4 Enter the interval, in hours, at which to want the Router to resynchronize with the SNTP Server, at the *Synchronization Interval* text box. The default is every 24 hours.
- 5 Select a primary SNTP server, and if required a secondary SNTP server from the appropriate drop down boxes.
- 6 If you want to enable daylight saving, check the *Daylight Savings* check box.
- 7 Select the month and day that you want daylight savings to begin at *Start Time*, and select the month and day that you want daylight savings to end at *End Time*.

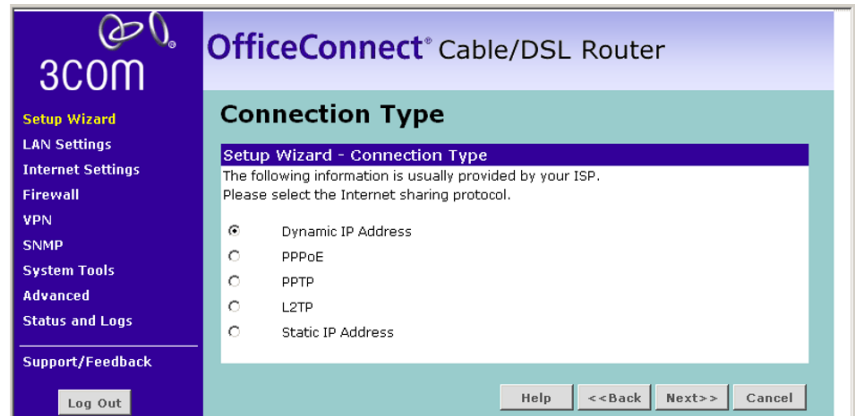


The Daylight Savings option advances the system clock by one hour between the dates that you specify in the Start Time and End Time drop

down lists. It does not cause the system clock to be updated for daylight savings time automatically.

- 8 Click *Next* to display the Connection Type screen.

Connection Type Figure 13 Connection Type Screen



This *Connection Type* screen allows you to set up the Router for the type of Internet connection you have. Before setting up your Internet connection mode, have the modem setting information from your ISP ready.

Select an Internet Addressing mode from the following:

- Dynamic IP Address — see [page 30](#).
- PPPoE (typically DSL users only) — see [page 31](#).
- PPTP (some DSL users in Europe) — see [page 32](#).
- L2TP (supported by some ISPs) — see [page 32](#).
- Static IP Address — see [page 34](#).

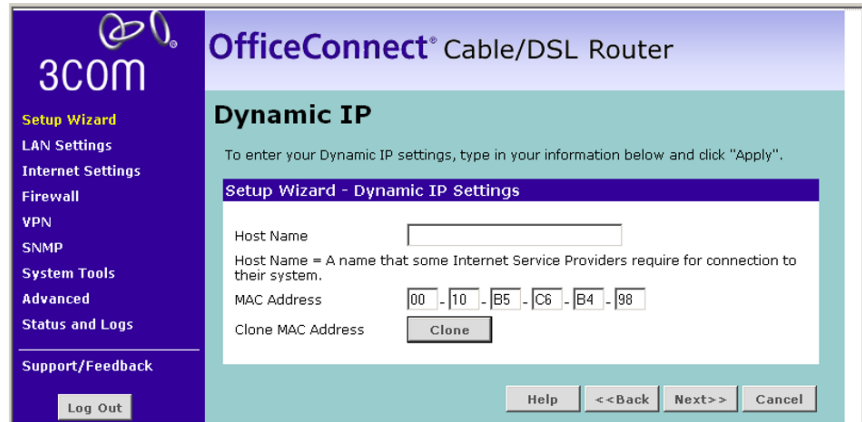
and click *Next*.



For further information on selecting a mode see [“Internet Settings”](#) on [page 42](#).

Dynamic IP Address Mode

Figure 14 Dynamic IP Screen



- 1 Some ISPs require a host name. If your ISP has this requirement, enter the host name in the *Host Name* text box .
- 2 Either:
 - If your ISP requires an assigned MAC address, enter the values for a *MAC address*. Or,
 - If the computer you are now using is the one that was previously connected directly to the cable modem, select *Clone*.
- 3 Click *Next*. The DNS screen displays. Refer to [“DNS”](#) on [page 35](#).

PPPoE Mode

Figure 15 PPPoE Interface Screen

3COM OfficeConnect® Cable/DSL Router

Setup Wizard

LAN Settings
Internet Settings
Firewall
VPN
SNMP
System Tools
Advanced
Status and Logs
Support/Feedback

PPPoE Interface

Setup Wizard - PPPoE Interface

User Name

Password

Retype Password

Service Name (Optional)

MTU (1200-1492)

Do not make changes to the MTU setting unless your ISP specifically requires a different setting than 1492.

Help <<Back Next>> Cancel

To setup the Router for use with a PPP over Ethernet (PPPoE) connection, do the following:

- 1 Enter your PPP over Ethernet user name in the *User Name* text box.
- 2 Enter your PPP over Ethernet password in the *Password* text box and enter it again in the *Retype Password* text box.
- 3 If required, enter your PPP over Ethernet service name in the *Service Name* text box. This is optional. Not all ISPs require a PPPoE service name.



Do not enter anything in this box if your ISP does not require a service name.

- 4 Enter the MTU value supplied by your ISP in the *MTU* text box. If your ISP has not supplied an MTU value, leave this at the default value. The default is 1454.
- 5 Check all of your settings, and then click *Next*. The DNS screen displays Refer to [“DNS”](#) on page [page 35](#).

PPTP Mode

Figure 16 PPTP Screen

The screenshot shows the 'Setup Wizard - PPTP Settings' screen for an OfficeConnect Cable/DSL Router. The interface includes a left-hand navigation menu with the following items: Setup Wizard (highlighted), LAN Settings, Internet Settings, Firewall, VPN, SNMP, System Tools, Advanced, Status and Logs, and Support/Feedback. A 'Log Out' button is located below the menu. The main content area is titled 'PPTP' and contains the following fields and options:

- PPTP Server:** A text box containing '0.0.0.0'.
- User ID:** An empty text box.
- Password:** An empty text box.
- Retype Password:** An empty text box.
- Idle Timeout:** A text box containing '10' with the note '(time in minutes; Enter 0 to never timeout)'.
- Get IP By DHCP:** A checked checkbox.
- IP Address:** Four separate text boxes for entering the IP address (0, 0, 0, 0).
- Subnet Mask:** Four separate text boxes for entering the subnet mask (0, 0, 0, 0).
- Default Gateway:** Four separate text boxes for entering the default gateway (0, 0, 0, 0).

At the bottom of the screen, there are four buttons: 'Help', '<< Back', 'Next >>', and 'Cancel'.

To setup the Router for use with a PPTP connection, use the following procedure:

- 1 Enter your PPTP server address in the *PPTP Server Address* text box.
- 2 Enter your PPTP user name in the *User ID* text box.
- 3 Enter your PPTP password in the *Password* text box, and enter it again in the *Retype Password* text box.
- 4 Type in an *Idle Timeout*. This is the amount of time you want the PPTP Server to remain inactive before the session is ended.
- 5 Either:
 - Check the *Get IP by DHCP* check box if you want to obtain the IP information from a DHCP Server on the network, or
 - If your ISP has provided you with IP address information, enter the *IP Address*, *Subnet Mask* and *Default Gateway* in the text boxes provided.
- 6 Check all of your settings, and then click *Next*. The DNS screen displays. Refer to [“DNS”](#) on [page 35](#).

L2TP

L2TP is supported by some Internet Service Providers (ISPs). Check with your ISP to make sure L2TP is supported before using this screen.

Figure 17 L2TP Screen

3COM OfficeConnect® Cable/DSL Router

L2TP

Type in the information provided by your ISP in the fields provided. When you have finished, click "Apply".

Setup Wizard - L2TP Settings

L2TP Server: 0.0.0.0

User ID: _____

Password: _____

Retype Password: _____

Idle Timeout: 10 (time in minutes; Enter 0 to never timeout)

Get IP by DHCP:

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Buttons: Help << Back Next >> Cancel

To setup the Router for use with an L2TP connection, do the following:

- 1 Enter your L2TP server address in the *L2TP Server* text box.
- 2 Enter your L2TP user name in the *User ID* text box.
- 3 Enter your L2TP password in the *Password* text box, and enter it again in the *Retype Password* text box.
- 4 Type in an *Idle Timeout*. This is the amount of time you want the L2TP Server to remain inactive before the session is ended.
- 5 Either:
 - Check the *Get IP by DHCP* check box if you want to obtain the IP information from a DHCP Server on the network, or
 - If your ISP has provided you with IP address information, enter the *IP Address*, *Subnet Mask* and *Default Gateway* in the text boxes provided.
- 6 Check all of your settings, and then click *Next*. The DNS screen displays. Refer to ["DNS"](#) on page [page 35](#).

Static IP Mode

Figure 18 Static IP Mode Screen

3COM OfficeConnect® Cable/DSL Router

Static IP

To enter your Static IP settings, type in your information below and click "Apply".

Setup Wizard - Static IP Settings

IP address assigned by your Service Provider

Subnet Mask

Service Provider Gateway Address

Help <<Back Next>> Cancel

Log Out

- 1 Enter the IP Address provided by your ISP in the *IP Address assigned by your Service Provider* text box.
- 2 Enter the Subnet Mask provided by your ISP in the *Subnet Mask* text box.
- 3 Enter the Gateway Address provided by your ISP in the *Service Provider Gateway Address* text box.
- 4 Check all of your settings, and then click *Next*.

DNS Figure 19 DNS Screen

To set up the Domain Name Server (DNS) information for your Router, do the following:

1 Either:

- Check the *Automatic from ISP* check box. Or,
- If your ISP has provided you with a specific DNS address to use type the *DNS Address* in the text box.

Optionally, you can type a *Secondary DNS Address* in the appropriate text box. Leave this box blank if your ISP has not supplied a secondary address.

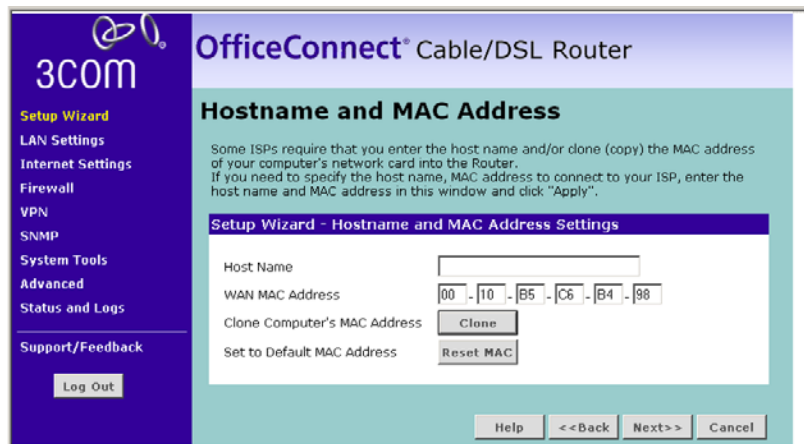
2 Click *Next* to display the Hostname and MAC Address screen.



If you selected the *Dynamic IP Address* option earlier in the Wizard, the LAN Settings screen now displays. Go to [“LAN Settings”](#) on [page 37](#).

Hostname and MAC Address

Figure 20 Hostname and MAC Address Screen



- 1 Some ISPs require a host name. If your ISP has this requirement, enter the host name in the *Host Name* text box.
- 2 Either:
 - If your ISP requires an assigned MAC address, enter the values for a *MAC address*. Or,
 - If the computer you are now using is the one that was previously connected directly to the cable modem, select *Clone*. Or,
 - To reset the MAC Address to the default, select *Reset MAC*.
- 3 Click Next to display the *LAN Settings* screen.

LAN Settings **Figure 21** LAN Settings Screen

LAN Configuration

This section of the screen displays a suggested LAN IP Address and Subnet Mask for the Router. It also allows you to change the IP address and subnet mask.

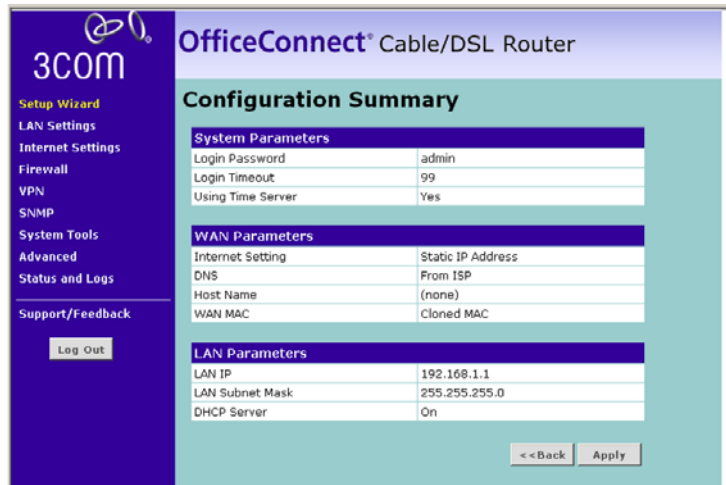
DHCP Server Parameters

The Router contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network. To set up the DHCP Server, do the following:

- 1 Activate the DHCP Server by clicking the *On* radio button.
- 2 Specify an IP Pool range in the *IP Pool Start Address* and *IP Pool End Address* text boxes. The largest available continuous IP pool will be automatically entered. If this is not appropriate, make the required changes.
- 3 Specify the DHCP Lease time by selecting the required value from the *Lease Time* drop down list. The lease time is the length of time the DHCP server will reserve the IP address for each computer.
- 4 If required, enter a *Local Domain Name*.
- 5 If you use 3Com NBX telephones, enter the IP address of the NBX call processor at *3Com NBX Call Processor*.
- 6 Click *Next* to display the Configuration Summary screen.

Configuration Summary

Figure 22 Configuration Summary Screen



When you complete the Setup Wizard, a configuration summary displays. Verify the configuration information of the Router and then click *Apply* to save your settings. 3Com recommends that you print this page for your records.

If you have made changes to the LAN Settings, you may need to reconfigure the computer you are using in order to make contact with the Router again.

Your Router is now configured and ready for use. See [Chapter 5](#) for a detailed description of the Router configuration screens.

5

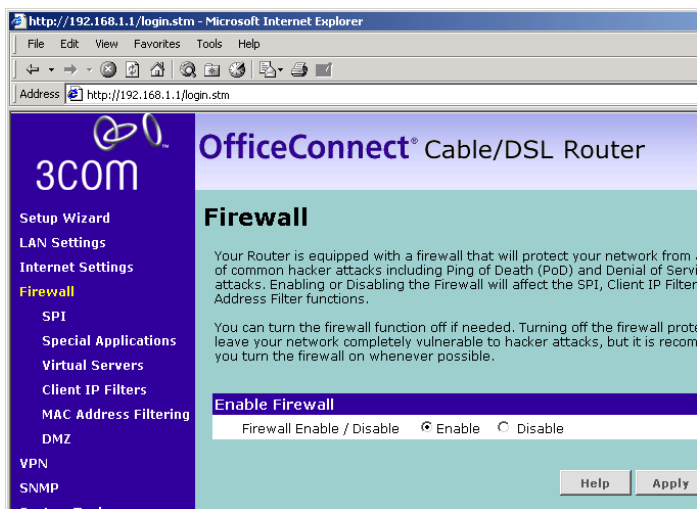
ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages

This chapter describes all the screens available through the Router configuration pages. To get to the configuration pages, browse to the Router by entering the URL in the location bar of your browser. The default URL is **http://192.168.1.1** but if you changed the Router LAN IP address during initial configuration, use the new IP address instead. When you have browsed to the Router, log in using your system password (default password is **admin**).

Main Menu

At the left side of all screens is a main menu, as shown in [Figure 23](#) on [page 40](#). When you click on a topic from the main menu, that screen displays. Some main menu topics, for example Firewall, also display a sub-menu; when you click on a sub-menu topic, that screen displays.

Figure 23 Main menu and Firewall sub-menu

LAN Settings

Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in most applications. If you need to make changes to the settings, you can do so.

The changes that you can make are:

- Change the Internal IP address of the Router. The default is 192.168.1.1
- Change the Subnet Mask. The default is 255.255.255.0
- Enable or Disable the DHCP Server Function. By default, DHCP is On (Enabled)
- Specify the Start and End IP Pool Address. The default is for the address range to start at 192.168.1.2 and end at 192.168.1.254
- Specify the IP address Lease Time. The default is half day
- If required, specify a local Domain Name
- If you use 3Com NBX telephones, specify an NBX call processor

The Router also provides you with a list of all client computers connected to the network. You can manage this list as described in [“DHCP Clients List”](#) on [page 42](#).

To configure the LAN Settings:

- 1 Select *LAN Settings* from the main menu to display the LAN Settings screen (Figure 24).

Figure 24 LAN Settings screen

LAN Settings

LAN Configuration

IP Address: 192 . 168 . 2 . 1
 Subnet Mask: 255 . 255 . 255 . 0

The DHCP server will assign an IP address to clients on LAN.

DHCP Server Parameters

DHCP server: On Off

IP Pool Start Address: 192 . 168 . 2 . 2
 IP Pool End Address: 192 . 168 . 2 . 254
 Lease Time: Two Days

Local Domain Name (Optional):
 3Com NBX Call Processor (Optional):

DHCP Client Lists

IP Address	Host Name	MAC Address	Fix	Configure
192.168.2.10		98-A4-F6-B5-F6-88	<input checked="" type="checkbox"/>	Edit Delete

Note: Only clients that have requested an IP address since the Router's last reboot and fixed associations are displayed in this list. Check Fix to fix an existing address, or click New to allocate an IP address to a MAC address.

- 2 Specify the Router *IP Address* and *Subnet Mask* in the appropriate fields. The default IP address of the Router is 192.168.1.1.
- 3 If you want to use the Router as a DHCP Server, select the *On* radio button.
- 4 If you need to, you can change the range of addresses allocated by the Router, by changing the *IP Pool Start Address* and *IP Pool End Address* text boxes.
- 5 Specify the DHCP Lease time by selecting the required value from the *Lease Time* drop down list. The lease time is the length of time the DHCP server will reserve the IP address for each computer
- 6 If required, specify the *Local Domain Name* for your network.
- 7 If you use 3Com NBX telephones, enter the IP address of the NBX call processor at *3Com NBX Call Processor*.
- 8 Either click *Apply* to save these settings, or go to DHCP Clients List if you want to manage the DHCP clients.

DHCP Clients List

The DHCP Clients List provides details on the devices that have received IP addresses from the Router. The list is only created when the Router is set up as a DHCP server. For each device that is connected to the LAN the following information is displayed:

- IP address — The Internet Protocol (IP) address issued to the client machine.
- Host Name — The client machine's host name, if configured.
- MAC Address — The Media Access Control (MAC) address of the client's network card.

From this screen, you can do the following:

- In the table, check the *Fix* text box to permanently fix the IP address.
- In the table, click *release* to release the displayed IP address.
- Click *New* to allocate an IP address to a MAC address.

As you connect more devices, the client list will grow to a maximum number of 253 clients.

Internet Settings

Before you can configure the Router, you need to know the IP information allocation method used by your ISP. There are five different ways that ISPs can allocate IP information, as described below:

Dynamic IP Address (DSL or Cable)

Dynamic IP addressing (or DHCP) automatically assigns the Router IP information. This method is popular with Cable providers. This method is also used if your modem has a built in DHCP server.

PPPoE (DSL only)

If the installation instructions that accompany your modem ask you to install a PPPoE client on your PC, then select this option. To configure the Router you will need to know the following:

- Username
- Password
- Service Name (if required by your ISP)
- MTU (if supplied by your ISP)



When you install the Router, you will not need to use the PPPoE software on your PC.

PPTP (DSL or Cable)

PPTP is only used by some European providers. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select this option. To configure the Router you will need to know the following:

- Username
- Password
- VPN Server address (usually your modem)



When you install the Router, you will not need to use the dialup VPN on your PC anymore.

L2TP (DSL or Cable)

L2TP is supported by some Internet Service Providers (ISPs). Check with your ISP to make sure L2TP is supported before selecting this option. To configure the Router you will need to know the following:

- Username
- Password
- L2TP Server address

Static IP Address (DSL or Cable)

The ISP provides the IP addressing information for you to enter manually. To configure the Router you will need to know the following:

- IP Address
- Subnet Mask
- ISP Gateway Address



These screens enable you to edit the settings that you configured using the Setup Wizard.

Connection to ISP

Before beginning this section, ensure you have the required information from your ISP.

Select *Internet Settings* from the main menu to display the Internet Settings screen. Then, select an IP allocation mode from the following:

- Dynamic IP Address (automatically allocated) — see [page 44](#).
- PPPoE (used by DSL providers only) — see [page 45](#)
- PPTP (used by some European providers) — see [page 46](#)
- L2TP (supported by some ISPs) — see [page 47](#)
- Static IP Address (to be specified manually) — see [page 48](#)

Dynamic IP Address

To configure the dynamic IP address connection for your Router:

- 1 Select *Dynamic IP Address* and then click *Next*. The Dynamic IP Screen displays (see [Figure 25](#)).

Figure 25 Internet Settings - Dynamic IP Screen

The screenshot shows the 'Dynamic IP' configuration screen for an OfficeConnect Cable/DSL Router. The left sidebar contains a navigation menu with 'Internet Settings' highlighted. The main area is titled 'Dynamic IP' and includes a sub-section 'Dynamic IP Settings'. Below this, there are three input fields: 'Host Name' (a text box), 'MAC Address' (a field containing '00-10-B5-C6-B4-98'), and 'Clone MAC Address' (a button labeled 'Clone'). At the bottom right of the main area are three buttons: 'Help', 'Apply', and 'Cancel'. The top of the screen displays the '3COM' logo and the router model 'OfficeConnect® Cable/DSL Router'.

- 2 Some ISPs require a host name. If your ISP has this requirement, enter the host name in the *Host Name* text box .
- 3 Either:
 - If your ISP requires an assigned MAC address, enter the values for a *MAC address*. Or,
 - If the computer you are now using is the one that was previously connected directly to the cable modem, select *Clone*.
- 4 Check all of your settings and then click *Apply*.

PPPoE

To configure the PPPoE connection for your Router:

- 1 Select *PPPoE* and then click *Next*. The PPPoE Interface screen displays (see [Figure 26](#)).

Figure 26 Internet Settings - PPPoE Interface Screen

- 2 Enter your PPP over Ethernet user name in the *User Name* text box.
- 3 Enter your PPP over Ethernet password in the *Password* text box and enter it again in the *Retype Password* text box.
- 4 If required, enter your PPP over Ethernet service name in the *Service Name* text box. This is optional. Not all ISPs require a PPPoE service name.



Do not enter anything in this box if your ISP does not require a service name.

- 5 Enter the MTU value supplied by your ISP in the *MTU* text box. If your ISP has not supplied an MTU value, leave this at the default value. The default is 1454.
- 6 Type in an *Idle Timeout*. This is the amount of time you want the PPPoE Server to remain inactive before the session is ended.
- 7 If you want to automatically reconnect to the server after timeout, check the *Auto Reconnect After Timeout* check box.
- 8 Check all of your settings, and then click *Apply*.

PPTP

To configure the PPTP connection for your Router:

- 1 Select *PPTP* and then click *Next*. The PPTP screen displays (see [Figure 27](#)).

Figure 27 Internet Settings - PPTP Screen

- 2 Enter your PPTP server address in the *PPTP Server Address* text box.
- 3 Enter your PPTP user name in the *User ID* text box.
- 4 Enter your PPTP password in the *Password* text box, and enter it again in the *Retype Password* text box.
- 5 Type in an *Idle Timeout*. This is the amount of time you want the PPTP Server to remain inactive before the session is ended.
- 6 Either:
 - Check the *Get IP by DHCP* check box if you want to obtain the IP information from a DHCP Server on the network.
With this check box enabled, you can click *Release* to release the WAN IP Address for the Router, or click *Renew* to renew the current WAN IP Address, using DHCP.

Or:

 - If your ISP has provided you with IP address information, enter the *IP Address*, *Subnet Mask* and *Default Gateway* in the text boxes provided, or
- 7 Check all of your settings, and then click *Apply*.

L2TP



Check with your ISP to make sure they support L2TP.

To configure the L2TP connection for your Router:

- 1 Select *L2TP* and then click *Next*. The L2TP screen displays (see [Figure 28](#)).

Figure 28 Internet Settings - L2TP Screen

The screenshot shows the 'L2TP' configuration screen on the OfficeConnect Cable/DSL Router. The interface includes a sidebar on the left with various settings categories. The main content area is titled 'L2TP' and contains a form with the following fields and controls:

- L2TP Server:** A text box containing '0.0.0.0'.
- User ID:** An empty text box.
- Password:** An empty text box.
- Retype Password:** An empty text box.
- Idle Timeout:** A text box containing '10' with the note '(time in minutes; Enter 0 to never timeout)'.
- Get IP By DHCP:** A checked checkbox with 'Renew' and 'Release' buttons next to it.
- IP Address:** A four-part dotted text box.
- Subnet Mask:** A four-part dotted text box.
- Default Gateway:** A four-part dotted text box.

At the bottom of the form are 'Help', 'Apply', and 'Cancel' buttons. A 'Log Out' button is located in the sidebar.

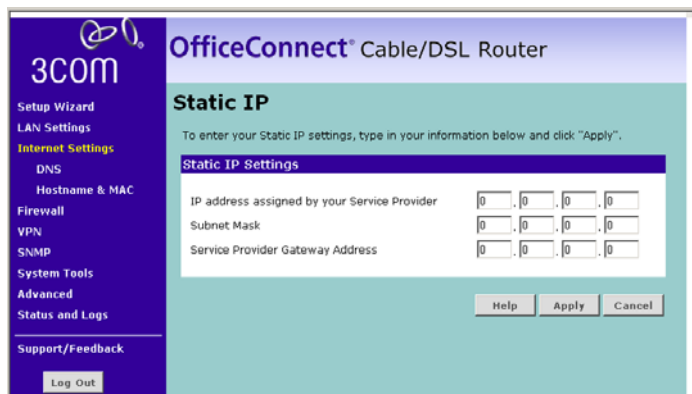
- 2 Enter your L2TP server address in the *L2TP Server* text box.
- 3 Enter your L2TP user name in the *User ID* text box.
- 4 Enter your L2TP password in the *Password* text box, and enter it again in the *Retype Password* text box.
- 5 Type in an *Idle Timeout*. This is the amount of time you want the L2TP Server to remain inactive before the session is ended.
- 6 Either:
 - Check the *Get IP by DHCP* check box if you want to obtain the IP information from a DHCP Server on the network.
With this check box enabled, you can click *Release* to release the WAN IP Address for the Router, or click *Renew* to renew the current WAN IP Address, using DHCP.
 - If your ISP has provided you with IP address information, enter the *IP Address*, *Subnet Mask* and *Default Gateway* in the text boxes provided.
- 7 Check all of your settings, and then click *Apply*.

Static IP Address

To configure a Static IP Address for your Router:

- 1 Select *Static IP Address* and then click *Next*. The Static IP Address screen displays (see [Figure 29](#)).

Figure 29 Internet Settings - Static IP Screen



The screenshot shows the configuration interface for a 3COM OfficeConnect Cable/DSL Router. On the left is a dark blue navigation menu with the 3COM logo and a 'Log Out' button at the bottom. The menu items are: Setup Wizard, LAN Settings, Internet Settings (highlighted in yellow), DNS, Hostname & MAC, Firewall, VPN, SNMP, System Tools, Advanced, Status and Logs, and Support/Feedback. The main content area has a light blue header with the text 'OfficeConnect Cable/DSL Router' and a sub-header 'Static IP'. Below the sub-header, there is a blue bar with the text 'Static IP Settings'. The main area contains the instruction: 'To enter your Static IP settings, type in your information below and click "Apply".' There are three rows of input fields: 'IP address assigned by your Service Provider', 'Subnet Mask', and 'Service Provider Gateway Address'. Each row has four individual input boxes for the octets of the IP address. At the bottom right of the form are three buttons: 'Help', 'Apply', and 'Cancel'.

- 2 Enter the IP Address provided by your ISP in the *IP Address assigned by your Service Provider* text box.
- 3 Enter the Subnet Mask provided by your ISP in the *Subnet Mask* text box.
- 4 Enter the Gateway Address provided by your ISP in the *Service Provider Gateway Address* text box.

Check all of your settings, and then click *Apply*.

DNS To configure the Domain Name Server (DNS) information for your Router, do the following:

- 1 Select *Internet Settings*, then from the sub-menu select *DNS*. The DNS screen displays (see [Figure 30](#)).

Figure 30 Internet Settings - DNS Screen

- 1 Either:

- Check the *Automatic from ISP* check box. Or,
- If your ISP has provided you with a specific DNS address to use, or you chose *Static IP Address* in the Internet Settings screen, type the *DNS Address* in the text box.

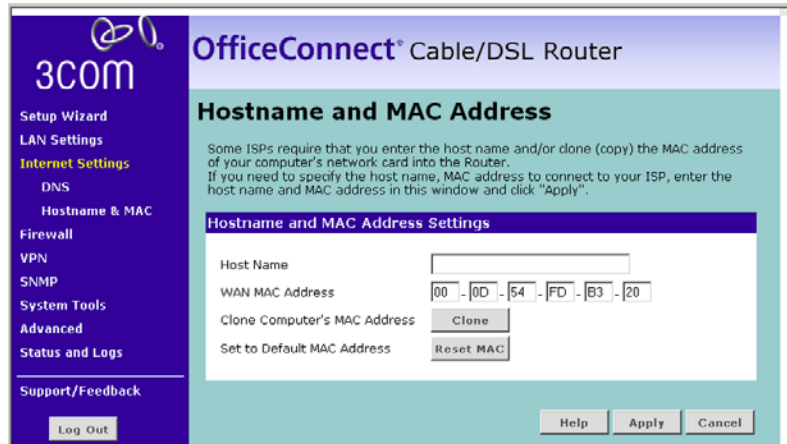
Optionally, you can type a *Secondary DNS Address* in the appropriate text box. Leave this box blank if your ISP has not supplied a secondary address.

- 2 Click *Apply* to save your settings.

Hostname & MAC To configure the Hostname and MAC Address information for your Router, do the following:

- 1 Select *Internet Settings*, then from the sub-menu select *Hostname & MAC*. The Hostname and MAC Address screen displays (see [Figure 31](#)).

Figure 31 Internet Settings - Hostname and MAC Address Screen



- 1 Some ISPs require a host name. If your ISP has this requirement, enter the host name in the *Host Name* text box.
- 2 Either:
 - If your ISP requires an assigned MAC address, enter the values for a *WAN MAC address*. Or,
 - If the computer you are now using is the one that was previously connected directly to the cable modem, select *Clone*. Or,
 - To reset the MAC Address to the default, select *Reset MAC*.
- 3 Click *Apply* to save the settings.

Firewall

Use the Firewall menu option to enable and disable the firewall, and to configure the following firewall functions

- SPI (Stateful Packet Inspection) — SPI inspects packets at the application layer, maintains TCP and UDP session information, and detects and prevents certain types of network attacks such as DoS attacks. See "[SPI](#)" on [page 51](#).

- Special Applications — Special Applications allows you to specify ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router. See [“Special Applications”](#) on [page 54](#).
- Virtual Servers — This function enables you to route external (Internet) calls for services such as a web server, FTP server, or other applications through your Router to your internal network. See [“Virtual Servers”](#) on [page 56](#).
- Client IP Filters — You can configure the Router to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers. See [“Client IP Filters”](#) on [page 57](#).
- MAC Address Filtering — This is a powerful security feature that allows you to specify which computers are allowed on the network. See [“MAC Address Filtering”](#) on [page 62](#).
- DMZ (De-Militarized Zone) — If you have a client PC that cannot run an Internet application properly from behind the firewall, you can use DMZ to open the client up to unrestricted two-way Internet access. See [“DMZ”](#) on [page 63](#).



CAUTION: DMZ reduces network security, and 3Com recommends you only use it on a temporary basis.

SPI Stateful Packet Inspection (SPI) inspects, and if required blocks packets at the application layer. SPI also maintains TCP and UDP session information, including timeouts and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as DoS attacks.



Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. The goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

To configure SPI information on your Router:

- 1 Select *Firewall* from the main menu, then select *SPI* from the sub-menu to display the SPI screen ([Figure 32](#) and [Figure 33](#)):

Figure 32 SPI Screen - upper section

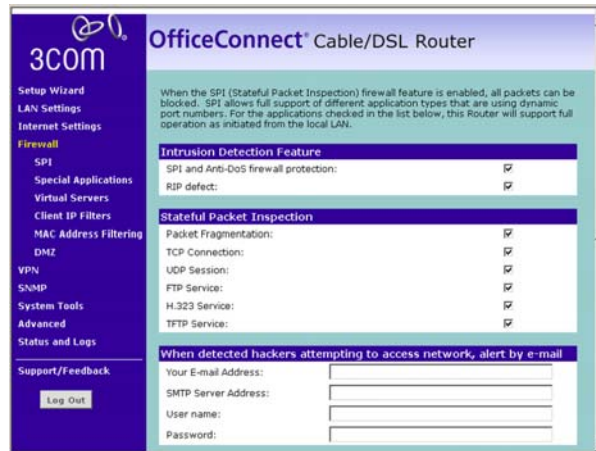
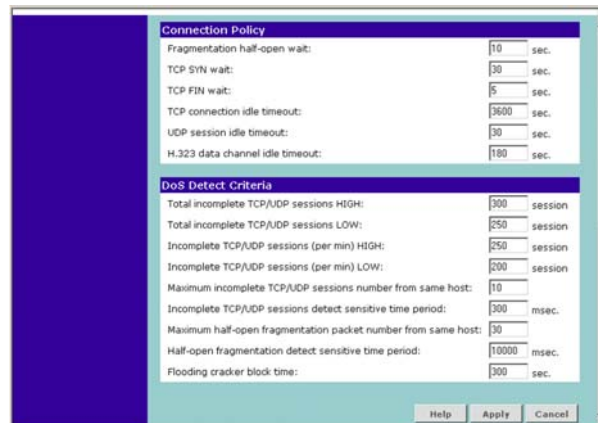


Figure 33 SPI Screen - lower section



Intrusion Detection Feature

The Intrusion Detection feature limits access for incoming traffic at the WAN ports.

- 2 Check the *SPI and Anti-DoS firewall protection* check box to enable SPI. When this feature is enabled, all incoming packets will be blocked except for those types that you allow in the Stateful Packet Inspection section.

- 3 If required, check the *RIP defect* check box. This feature stops unacknowledged packets from accumulating in the input queue.

Stateful Packet Inspection

- 4 The Stateful Packet Inspection section displays a list of traffic types. If you leave the check box for a traffic type blank, this traffic type is blocked. If you check the check box, the Router allows this type of incoming traffic, but only if the connection was initiated from the local LAN.

For example, if you check only the *FTP Service* check box, all incoming traffic is blocked except for FTP connections initiated from the local LAN.

Alert by E-mail

- 5 In the *Your E-mail Address* text box, enter the e-mail address you want alerts to be sent in the event of a hacker attack.
- 6 Enter your *SMTP Server Address*.
- 7 Enter your SMTP Server *User Name*.
- 8 Enter your SMTP Server *Password*.

Connection Policy

- 9 In the *Fragmentation half-open wait* text box, enter the length of time, in seconds, that you want an unassembled packet to remain active before the Router drops it. The default is 10 seconds.
- 10 In the *TCP SYN wait* text box, enter the length of time, in seconds, that you want the Router to wait for a TCP session to synchronize before it drops the session. The default is 30 seconds.
- 11 In the *TCP FIN wait* text box, enter the length of time, in seconds, that you want a TCP session to remain active after the Router detects a FIN packet. The default is 5 seconds.
- 12 In the *TCP connection idle timeout* text box, enter the length of time, in seconds, that you want a TCP session to remain active if there is no activity. The default is 3600 seconds (1 hour).
- 13 In the *UDP session idle timeout* text box, enter the length of time, in seconds, that you want a UDP session to remain active if there is no activity. The default is 30 seconds.
- 14 In the *H.323 data channel idle timeout* text box, enter the length of time, in seconds, that you want an H.323 session to remain active if there is no activity. The default is 180 seconds.

DoS Detect Criteria

- 15 In the *Total incomplete TCP/UDP sessions HIGH* text box, enter the number of unestablished sessions that will cause the software to start deleting half-open sessions. The default is 300.
- 16 In the *Total incomplete TCP/UDP sessions LOW* text box, enter the number of unestablished sessions that must be reached before the software stops deleting half-open sessions. The default is 250.
- 17 In the *Incomplete TCP/UDP sessions (per min) HIGH* text box, enter the maximum number of incomplete TCP/UDP sessions allowed per minute. The default is 250 sessions.
- 18 In the *Incomplete TCP/UDP sessions (per min) LOW* text box, enter the minimum number of incomplete TCP/UDP sessions allowed per minute. The default is 200 sessions.
- 19 In the *Maximum incomplete TCP/UDP sessions number from the same host* text box, enter the maximum number of incomplete sessions allowed from the same host. The default is 10 sessions.
- 20 In the *Incomplete TCP/UDP sessions detect sensitive time period* text box, enter the length of time that must elapse before an incomplete TCP/UDP session is detected as incomplete. The default is 300 msec.
- 21 In the *Maximum half-open fragmentation packet number from the same host* text box, enter the maximum number of half-open fragmentation packets allowed from the same host. The default is 30 packets.
- 22 In the *Half-open fragmentation detect sensitive time period* text box, enter the length of time that must elapse before a half-open fragmentation session is detected as half-open. The default is 10000 msec.
- 23 In the *Flooding cracker block time* text box, enter the length of time that must elapse between detection of a flood attack and blocking the attack. The default is 300 seconds.
- 24 Click *Apply* to save the settings.

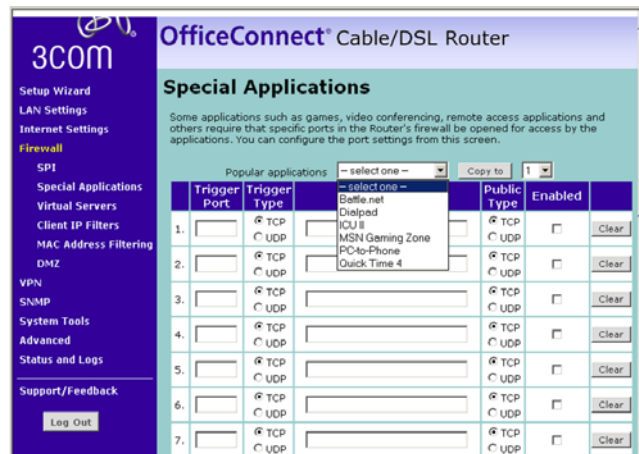
Special Applications

Special Applications let you choose specific ports, and for these ports to choose the specific applications that you want to work with the Network Address Translation (NAT) feature of the Router. You can either choose from a list of applications, or configure another application using information supplied by the application vendor.

To set up one of the listed Special Applications on your Router, do the following:

- 1 Select *Firewall* from the main menu, then select *Special Applications* from the sub-menu. The Special Applications screen displays (Figure 34).

Figure 34 Special Application Screen



- 2 Select an application from the *Popular Applications* drop-down list.
- 3 Select the row that you want to copy the settings to from the *Copy To* drop-down list, and click on *Copy To*. The settings will be transferred to the row you specified.
- 4 Click *Apply* to save the setting for that application.

If the application you want to configure is not listed, you will need to check with the application vendor to determine which ports need to be configured. You can then manually input this port information into the Router. To do this:

- 1 Specify the trigger port (the one used by the application when it is initialized) in the *Trigger Port* column, and specify whether the trigger is TCP or UDP in the *Trigger Type* column.
- 2 Specify the public ports used by the application in the *Public Port* column. These are the ports that will need to be opened up in the firewall for the application to work properly, . Also specify whether these ports are TCP or UDP in the *Public Type* column.
- 3 If required, temporarily enable or disable an entry in the table by checking or unchecking the *Enabled* checkbox.

- 4 Click *Apply* to save the setting for this application.

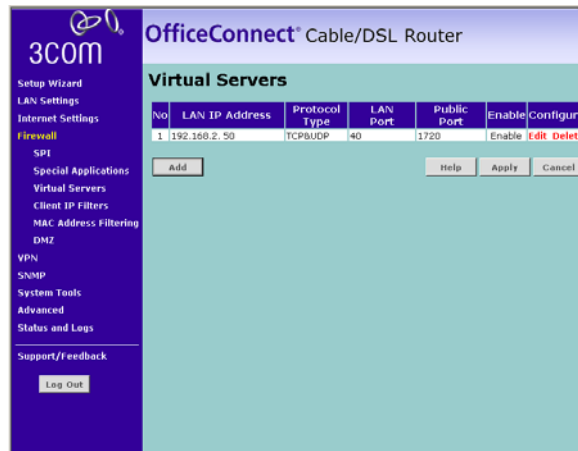
Virtual Servers This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be 'seen'.

If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

To manually enter Virtual Server settings, do the following:

- 1 Select *Firewall* from the main menu, then select *Virtual Servers* from the sub-menu. The Virtual Servers screen displays (Figure 35)

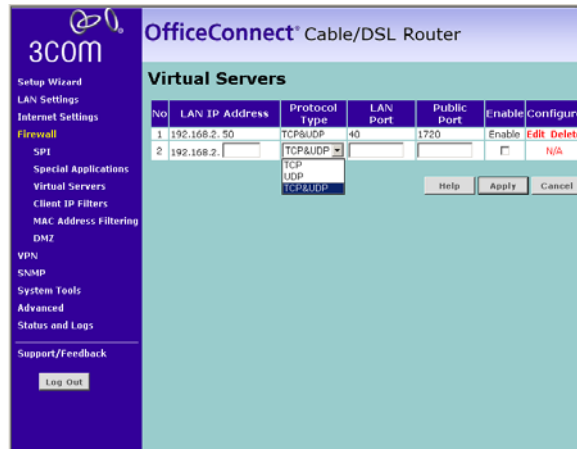
Figure 35 Virtual Server Screen



- 2 Click *Add* to configure a new Virtual Server entry, or click *Edit* in the Configure column to edit an existing entry. The Virtual Server - Add/Edit screen displays (Figure 36).



You can delete an existing entry by clicking on delete in the Configure column.

Figure 36 Virtual Server - Add/Edit Screen

- 3** Enter the IP address of the internal machine in the *LAN IP Address* text box.
- 4** Select a protocol type (TCP, UDP or both) from the *Protocol Type* drop-down list.
- 5** Enter the LAN Port which the traffic will be routed to in the *LAN Port* text box.
- 6** Enter the Public port that will be seen by clients on the Internet in the *Public Port* text box.
- 7** Check the *Enable* check box to activate this Virtual Server.
- 8** Click *Apply* to save this Virtual Server entry.

Client IP Filters This sub-menu option displays three tabs along the top of the main screen: *Access Control*, *URL Filter*, and *Schedule Rule*. Each of these tabs displays a screen that enables you to configure a client IP filter function.

Access Control

Access Control allows you to define the types of traffic permitted or not permitted to and from the Internet.

To configure Access Control, do the following:

- 1 Select *Firewall* from the main menu, then select *Client IP Filters* from the sub-menu, and make sure the *Access Control* tab is selected. The *Access Control* screen displays (Figure 37).

Figure 37 Access Control Screen



- 2 At the Enable Filtering Function radio buttons, select *Enable* or *Disable* to enable or disable all Access Control rules.
- 3 Click *Apply* to save the settings.

To control access to specific Internet services:

- 1 Click on *Add PC*, or click *Edit* in the Configure column to edit an existing entry. The Access Control - Add PC screen displays (Figure 38).

Figure 38 Access Control - Add PC Screen

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	<input type="checkbox"/>
Enable URL Filter	HTTP (Ref. URL Filter Page)	<input type="checkbox"/>
Enable Content Filter	HTTP (Ref. Content Filter Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port: 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port: 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port: 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port: 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port: 21	<input type="checkbox"/>

- 2 Enter a description for the filter you are defining in the *Client PC Description* field.
- 3 Enter the IP address or IP address range into the *Client IP Address* fields.
- 4 Select the services to be blocked. A list of popular services is given on this screen; to block a particular service place a check in the appropriate *Blocking* checkbox.

If the service to be restricted is not listed on the screen, you can enter a custom range of ports at the bottom of the page, under *User Defined Blocked Ports*.

- 5 If you want the restriction to only apply at certain times, select the schedule rule to apply from the *Schedule Rule* drop down list.

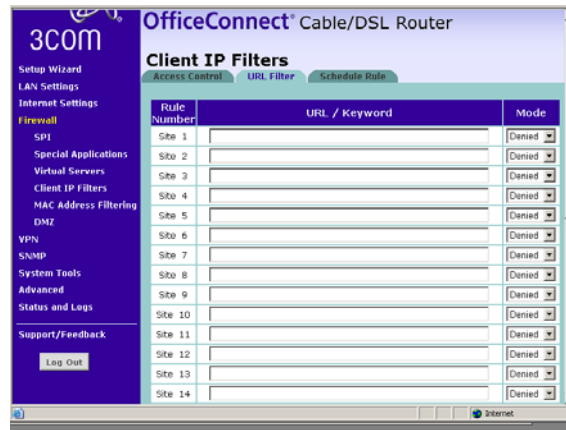


Schedule Rules are defined on the *Schedule Rule* screen (see "[Schedule Rule](#)" on page 60).

- 6 Click *Apply* to save the settings.

URL Filter

Select the *URL Filter* tab to specify the web sites or keywords that you want to filter on your network. The URL Filter screen displays (Figure 39).

Figure 39 URL Filter Screen

To configure URL Filtering, do the following:

- 1 Enter the URLs or keywords to be allowed or blocked in the URL/Keyword column.
- 2 Select either Denied or Allowed from the Mode drop-down list to deny or allow access to web site containing these words.

For example, entering a keyword of "sex" would block access to any URL that contains the string "sex". However, this would also filter the following URLs:

- **www.sussex.com**
- **www.thisexample.com**

Therefore, choose the words and phrases to be blocked or allowed carefully.

- 3 Click *Apply* to save the settings.

For URL Filtering to work, you will need to make sure that URL filtering is enabled for each client PC in the "Access Control" screen. To do this:

- In the Access Control - Add PC screen ([Figure 38](#)), check the *Blocking* check box for *Enable URL Filter* to activate the URL filtering specified in the URL Filter table. See "[Access Control](#)" on [page 57](#).

Schedule Rule

You can configure the Router to restrict access to the Internet, e-mail or other network services at specific days and times. The schedule rules that

you set up here are available for selection when you configure access control (see [“Access Control”](#) on [page 57](#)).

To configure a schedule rule, do the following:

- 1 Select *Firewall* from the main menu, then select *Client IP Filters* from the sub-menu, and select the *Schedule Rule* tab. The *Schedule Rule* screen displays ([Figure 40](#)).

Figure 40 Schedule Rule Screen



- 2 Click *Add Rule*, or click *Edit* in the *Configure* column to edit an existing entry. The *Schedule Rule - Add Rule* screen displays ([Figure 41](#)).



You can delete an existing entry by clicking on *delete* in the *Configure* column.

Figure 41 Schedule Rule - Add Rule Screen

OfficeConnect® Cable/DSL Router

Client IP Filters

Access Control | IP Filter | Schedule Rule

Enter the fields for this schedule rule.

Edit Schedule Rule

Name:

Comment:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

Help Apply Cancel

- 3 Enter a name and comment for the schedule rule in the *Name* and *Comment* text boxes.
- 4 Specify the schedule rules for the required days and times. Note that all times should be in 24 hour format.
- 5 Click *Apply* to save the settings.

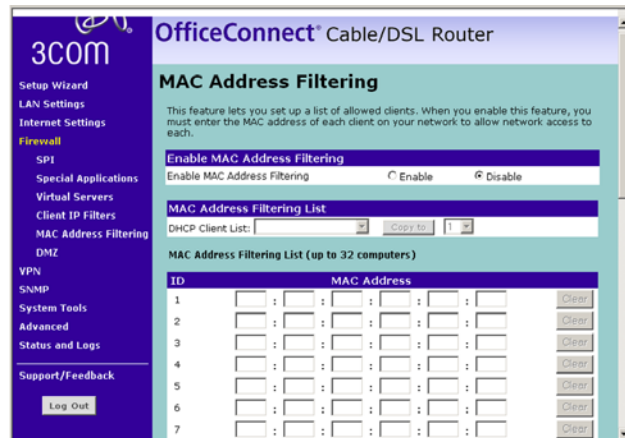
MAC Address Filtering

The MAC Address Filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computers attempting to access the network that are not specified in the filter list will be denied access.

To set up MAC Address Filtering, do the following:

- 1 Select *Firewall* from the main menu, then select *MAC Address Filtering* from the sub-menu. The *MAC Address Filtering* screen displays (Figure 42).

Figure 42 MAC Address Filtering



- 2 To enable this feature, click the *Enable* radio button.
- 3 Enter the MAC address of each client on your network that you want to allow network access in the *MAC Address* text boxes.

Alternatively, you can copy a MAC address into the *MAC Address* text box, as follows:

- a Select the name of the computer from the *DHCP Client List*
 - b Select a row ID from the *Copy To* drop-down list
 - c Click on *Copy To*. The MAC address is inserted into the selected row.
- 4 Click *Apply* to save the settings.

DMZ If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application.

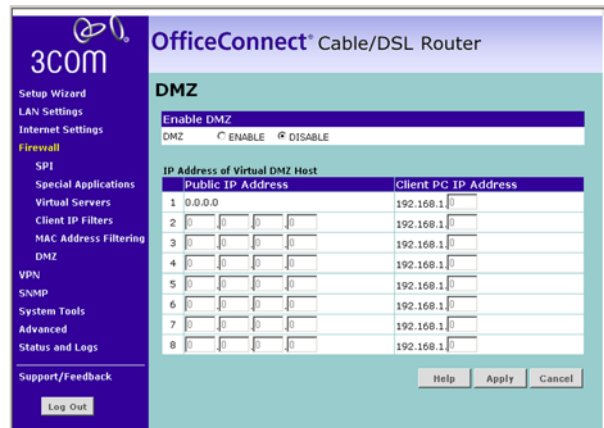


CAUTION: Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ, do the following:

- 1 Select *Firewall* from the main menu, then select *DMZ* from the sub-menu. The *DMZ* screen displays (Figure 43).

Figure 43 DMZ Screen



- 2 Select the *ENABLE* radio button.
- 3 The first row in the *Public IP Address* column defaults to the IP address of the WAN interface. Enter the last digits of the client PCs IP address in the *Client PC IP Address* text box.
- 4 If you have been assigned more than one IP address for the WAN interface, then you can enter up to eight different IP addresses in the *Public IP Address* text boxes.
- 5 For each Public IP Address, enter a client PCs IP address in the *Client PC IP Address* text box.
- 6 Click *Apply* to save the settings.

VPN

The Router has a Virtual Private Network (VPN) feature that provides a secure link between remote users and the corporate network by establishing an authenticated and encrypted tunnel for passing secure data over the Internet. The Router supports three modes of VPN operation:

- IPsec (IP Security) — provides IP network-layer encryption. IPsec can support large encryption networks (such as the Internet) by using digital certificates for device authentication. When setting up an IPsec

connection between two devices, make sure that they support the same encryption method.



Enabling IPsec VPN disables pass-through to IPsec and L2TP over IPsec Virtual Servers on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.

- PPTP (Point-to-Point Tunneling Protocol) — provides a secure tunnel for remote client access to a PPTP security gateway. It is not as secure as IPsec but is easy to administer. PPTP does not support gateway to gateway connections and is only suitable for connecting remote users. Check that your ISP's routers support this protocol before you use it.



Enabling the PPTP Server disables PPTP pass-through to a Virtual Server on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.

- L2TP over IPsec — this is a combination of two protocols. L2TP is used to authenticate a user, and IPsec is used to encrypt data. L2TP over IPsec does not support gateway to gateway connections and is only suitable for connecting remote users. Check that your ISP's routers support this protocol before you use it.



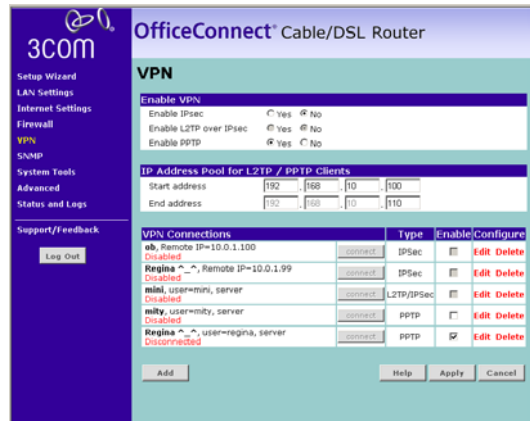
Enabling L2TP over IPsec disables pass-through to IPsec and L2TP over IPsec Virtual Servers on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.

Using the VPN Tunnel Configuration screen, you can add new IPsec, L2TP over IPsec and PPTP connections, and to edit existing connections. When adding or editing values on this screen remember that both ends of the connection must contain the same information.

To configure a VPN connection on your Router:

- 1 Select *VPN* from the main menu. The *VPN* screen displays (Figure 44).

Figure 44 VPN Screen



- 2 In the *Enable VPN* section, select the *Yes* radio button for the connection methods you want to use.



IPSec must be enabled if you want to use L2TP over IPSec.

- 3 To set up the Router for L2TP and PPTP, you must allocate IP addresses from the Router's LAN for use with the protocol. The connections made by L2TP and PPTP will appear to come from these addresses. The addresses must be in a continuous range.

In the *IP Address Pool for L2TP/PPTP Clients* section, enter the first LAN address in the range in the *Start Address* text boxes, and the last address in the range in the *End Address* text boxes.



These addresses must be within the Router's LAN subnet, and must not form part of the DHCP pool.

- 4 The *VPN Connections* table displays the currently configured VPN connections. Refer to one of the following sections for details on how to set up or edit a VPN connection:
 - [“Adding an IPSec Connection”](#) on [page 67](#).
 - [“Adding an L2TP over IPSec Connection”](#) on [page 68](#).
 - [“Adding a PPTP Connection”](#) on [page 70](#).

Adding an IPSec Connection

To add an IPSec Connection, or to edit an existing IPSec connection:

- 1 In the VPN screen, click *Add*, or click *Edit* to edit an existing connection.
- 2 At the *Tunnel Type* drop-down list, select *IPSec*. The screen shown in [Figure 45](#) displays.


Figure 45 VPN Tunnel Configuration - IPSec Screen

- 3 Enter a descriptive name for the tunnel at the *Tunnel Name* text box.
- 4 At the *Remote VPN Server* drop-down list, select either *IP Address* or *ANY*. If you select *IP Address*, enter the IP address or host name of the remote server in the *IP Address/Host Name* text box. If you select *ANY*, you do not need to specify an IP address or host name, as any remote server can be used.
- 5 At the *Remote Party ID* drop-down list, select either *IP_IPV4_ADDR* or *ID_USER_FQDN*. This must be entered identically on the IPSec software installed on the client's machine.



If you select IKE Main Mode from the Key Management drop-down list (see [step 8](#)), you must enter IP_IPV4_ADDR here.

- 6 Type a name for the *Remote Party ID* in the text box next to the drop-down list. This must be unique for each connection rule that you create.
- 7 Enter the *Remote Network Address* and *Remote Subnet Mask* for the Remote Party ID. The remote network address is usually the network address of the LAN connected to the remote server.

- 8 Enter the *Network Address* and *Subnet Mask* of the local secure group. The network address of the local secure group is usually the network address of the local network. From the *Key Management* drop-down list, select either IKE Main Mode or IKE Aggressive Mode.
 - 9 At the *Pre-shared Key* text box, enter the password for the connection. This must be unique for each connection rule that you create.
 - 10 Enter the *Key lifetime*, in seconds. The default is 3600 seconds. The value must be at least 300 seconds.
 - 11 Select MD5, SHA1 or None from the *Authentication Algorithm* drop-down list. Both ends of the connection must use the same value.
 - 12 Select DES, 3DES or None from the *Encrypt Algorithm* drop-down list. 3DES is more secure than DES but may take longer to encrypt. Both ends of the connection must use the same value.
-  *3DES is not shipped as standard with the Router due to international restrictions on encryption. If your country permits their use, they can be downloaded from the 3Com Web site at <http://www.3com.com>*
- 13 Click *Apply* to save the settings.

 *The IKE Keep Alive feature is not available.*

Adding an L2TP over IPsec Connection

To add an L2TP over IPsec Connection, or to edit an existing L2TP over IPsec connection:

- 1 In the VPN screen, click *Add*, or click *Edit* to edit an existing connection.
- 2 At the *Tunnel Type* drop-down list, select *L2TP over IPsec*. The screen shown in [Figure 46](#) displays.

Figure 46 VPN Tunnel Configuration - L2TP over IPsec Screen

- 3 Enter a name for the tunnel at the *Tunnel Name* text box.
- 4 Enter the user name that the remote VPN client will use to connect in the *User name* text box.
- 5 Enter the password that will need to be supplied to connect in the *Password* text box.
- 6 Type in an *Idle Timeout*. This is the amount of time, in minutes, that you want the connection to remain inactive before it times out. Enter 0 if you do not want the connection to timeout.
- 7 Select either the *L2TP Server* or *L2TP Client* radio button. If you select *L2TP Client*, enter the following information:
 - Check the *Auto reconnect* check box if you want to automatically re-connect if the session ends or is dropped.
 - Select either *Network* or *Host* as the local type setting.
 - Enter the *Remote Server* address in the text box.
- 8 If you want to enter details of the remote network, check the *Remote Network Setting - Enable* check box, then enter the *Remote Network Address* and *Remote Subnet Mask*. This information must be entered if you want to see clients connected to the *L2TP over IPsec* server.
- 9 At the *Pre-shared Key* text box, enter the password for the *IPsec* connection. This must be unique for each connection rule that you create.
- 10 At the *Remote Party ID* drop-down list, select either *IP_IPV4_ADDR* or *ID_USER_FQDN*.

- 11 Type a name for the Remote Party ID in the text box next to the drop-down list. This must be unique for each connection rule that you create.
- 12 Click *Apply* to save the settings.

Adding a PPTP Connection

To add a PPTP Connection, or to edit an existing PPTP connection:

- 1 In the VPN screen, click *Add*, or click *Edit* to edit an existing connection.
- 2 At the *Tunnel Type* drop-down list, select *PPTP*. The screen shown in [Figure 47](#) displays.

Figure 47 VPN Tunnel Configuration - PPTP Screen

The screenshot shows the 'VPN Tunnel Configuration - PPTP' screen on a 3COM OfficeConnect Cable/DSL Router. The left sidebar contains navigation options: Setup Wizard, LAN Settings, Internet Settings, Firewall, VPN (highlighted), SNMP, System Tools, Advanced, Status and Logs, and Support/Feedback. The main content area is titled 'VPN Tunnel Parameters - PPTP' and includes the following fields and options:

- Tunnel Type:** A drop-down menu set to 'PPTP'.
- Tunnel Name:** An empty text box.
- User name:** An empty text box.
- Password:** An empty text box.
- Idle Timeout:** A text box containing '10' with the note '(time in minutes; Enter 0 to never timeout)'.
- PPTP Type Setting:** Two radio buttons: 'PPTP Server' (unselected) and 'PPTP Client' (selected).
- Local Type Setting:** Two radio buttons: 'Network' (selected) and 'Host' (unselected).
- Remote Server IP:** A text box containing '0.0.0.0'.
- Remote Network Setting:** A checkbox labeled 'Enable' which is checked.
- Remote Network Address:** Four text boxes for IP address (0, 0, 0, 0).
- Remote Subnet Mask:** Four text boxes for subnet mask (0, 0, 0, 0).

At the bottom right, there are three buttons: 'Help', 'Apply', and 'Cancel'.

- 3 Enter a name for the tunnel at the *Tunnel Name* text box.
- 4 Enter the user name that the remote VPN client will use to connect in the *User name* text box.
- 5 Enter the password that will need to be supplied to connect in the *Password* text box.
- 6 Type in an *Idle Timeout*. This is the amount of time, in minutes, that you want the connection to remain inactive before it times out. Enter 0 if you do not want the connection to timeout.
- 7 Select either the *PPTP Server* or *PPTP Client* radio button. If you select PPTP Client, enter the following information:
 - Check the *Auto reconnect* check box if you want to re-connect automatically after the PPTP session ends or is dropped.

- Select either *Network* or *Host* as the local type setting.
 - Enter the *Remote Server IP* address in the text box.
- 8 If you want to enter details of the remote network, check the *Remote Network Setting - Enable* check box, then enter the *Remote Network Address* and *Remote Subnet Mask*.
 - 9 Click *Apply* to save the settings.

SNMP

SNMP (Simple Network Management Protocol) allows remote management of your Router by a PC that has an SNMP management agent installed.

You can configure the following SNMP parameters:

- Community — This configures the SNMP community string, which authenticates remote users.
- Trap — You can also configure the Router to send status messages to the SNMP management agent if a problem occurs on the network. This is done by using Traps.

To set up SNMP Community and Trap parameters, do the following:

- 1 Select *SNMP* from the main menu. The *SNMP* screen displays ([Figure 48](#)).

Figure 48 SNMP Screen

The screenshot shows the 'OfficeConnect Cable/DSL Router' interface. On the left is a navigation menu with 'SNMP' selected. The main area is titled 'SNMP' and contains the following configuration options:

Enable SNMP
 Enable SNMP Enable Disable

Please enter the SNMP Community parameters in the following table.

No.	Community	Access	Valid
1	public	Read	<input checked="" type="checkbox"/>
2	private	Write	<input checked="" type="checkbox"/>
3		Read	<input type="checkbox"/>
4		Read	<input type="checkbox"/>
5		Read	<input type="checkbox"/>

Please enter the SNMP Trap parameters in the following table.

No.	IP Address	Community	Version
1		Disabled
2		Disabled
3		Disabled
4		Disabled

- 2 Select *Enable* to activate SNMP.

- 3 In the *Community* column, enter the name of the SNMP communication channel. Your SNMP management agent needs to be configured with this name so that it can communicate with your Router.
- 4 In the *Access* column, select either:
 - *Read* to allow the management agent to collect data (for example, bandwidth usage) from your Router. Or,
 - *Write* to allow the management agent to change the configuration of your Router.
- 5 Check the *Valid* check box to enable the community.
- 6 If you do not want to configure your Router to send status messages to the SNMP management agent if a problem occurs, click *Apply* to save the settings.

If you want to configure your Router to send status messages, or Traps, configure SNMP Traps in the lower section of the screen as follows:
- 7 In the *IP Address* field, enter the IP address of the PC to which you want your Router to send status messages.
- 8 In the *Community* field, enter the community that you want to use to access status messages.
- 9 Select the version of trap messaging that your management agent supports from the *Version* drop-down list. The Router supports *V1* and *V2c* trap messaging.
- 10 Click *Apply* to save the settings.

System Tools

These screens enable you to manage different parameters of the Router and perform administrative functions. The Systems Tools menu has the following sub-menus:

- **Restart Router** — enables you to restart the Router and retain the current system configuration.
- **Reset to Factory Defaults** — resets the Router to factory default settings, and loses the current configuration.
- **Backup/Restore Settings** — enables you to save a configuration file, and restore any saved configuration file.
- **Upgrade** — enables you to upgrade the Router's firmware.
- **Admin Password** — enables you to reset the system password.
- **Time Zone** — enables you to change time zone settings.

Refer to the following sections for details on each of these options.

Restart Router Sometimes it may be necessary to restart or reboot the Router. Restarting or rebooting the Router will not delete any of your configuration settings.

To restart the Router:

- 1 Select *System Tools* from the main menu, then select *Restart* from the sub-menu. The Restart Router screen displays ([Figure 49](#)).

Figure 49 Restart Router Screen



- 2 Click *Restart* to restart Router.

Reset to Factory Defaults Use this option to reset all of the configuration settings in the Router to the factory (default) settings.



CAUTION: 3Com recommends that you backup your configuration settings before you reset to factory defaults, otherwise configuration information may be lost. Refer to ["Backup/Restore Settings"](#) on [page 74](#) for details.

To restore the factory default settings:

- 1 Select *System Tools* from the main menu, then select *Reset to Factory Defaults* from the sub-menu. The Reset to Factory Defaults screen displays (Figure 50).

Figure 50 Reset to Factory Defaults Screen



- 2 Click *Reset*.

Backup/Restore Settings

You can save your current configuration using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed.



3Com recommends that you backup your current configuration before performing a firmware update or a reset to factory defaults.

This option also enables you to restore a previously saved configuration.

Saving a configuration file

To save a configuration file:

- 1 Select *System Tools* from the main menu, then select *Backup/Restore Settings* from the sub-menu. The *Backup/Restore Settings* screen displays ([Figure 51](#)).

Figure 51 Backup/Restore Settings Screen



- 2 Click *Save* to save your current configuration settings.

Restoring a configuration file

To restore a previously saved configuration file:

- 1 Select *System Tools* from the main menu, then select *Backup/Restore Settings* from the sub-menu. The *Backup/Restore Settings* screen displays ([Figure 51](#)).
- 2 Click *Browse* to display the list of currently saved configuration files. The file you select displays in the text box.
- 3 Click *Restore* to restore this configuration file.

Upgrade From time to time 3Com may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may exist with the current version.

Please download the firmware file to your PC first, and then use the Upgrade screen to upload the firmware to the Router.

To upload a firmware file from your PC to your Router:

- 1 Select *System Tools* from the main menu, then select *Upgrade* from the sub-menu. The *Upgrade* screen displays (Figure 52).

Figure 52 Upgrade Screen



- 2 Click *Browse* to display the list of currently saved firmware upgrade files. The file you select displays in the text box.
- 3 Click *Upgrade* to upload this firmware file to your Router.

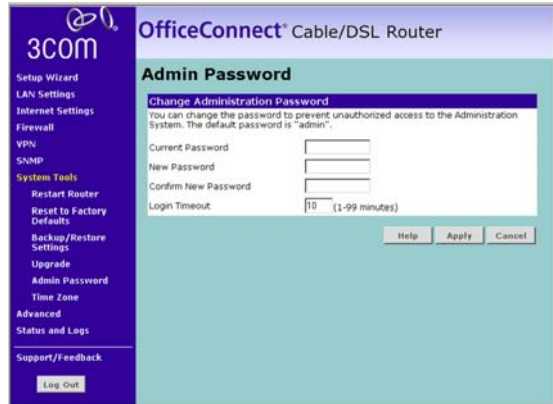
Admin Password

The Router ships with a default password of *admin*. 3Com recommends that you change the password for added security. Keep your password in a safe place as you will need this password to log in to the Router in the future. 3Com also recommends that you set a password if you plan to use the Remote management feature of this Router.

To change the password:

- 1 Select *System Tools* from the main menu, then select *Admin Password* from the sub-menu. The *Admin Password* screen displays (Figure 53).

Figure 53 Admin Password Screen



- 2 Enter the current password into the *Current password* text box.
- 3 Enter the new password into the *New Password* and *Confirm New Password* fields.
- 4 Type in a *Login Timeout*. This is the amount of time you want the Router to remain inactive before it returns to the login screen. The default is 10 minutes.
- 5 Click *Apply*.

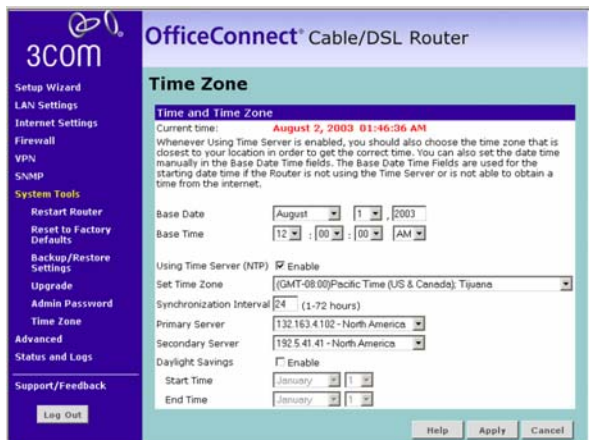
Time Zone The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the Internet. The synchronized clock in the Router is used to record the security log and control client filtering.

You can specify which SNTP servers the Router will use to update its system clock, although doing this should only be necessary if you are experiencing difficulty.

To configure time zone settings:

- 1 Select *System Tools* from the main menu, then select *Time Zone* from the sub-menu. The *Time Zone* screen displays (Figure 54).

Figure 54 Time Zone Screen



- 2 Select the *Base Date* and *Base Time*. The Router will use these settings if it is unable to connect to the Internet or SNTP Server.
- 3 To enable SNTP, check the *Using Time Server (NTP)* check box.
- 4 Select a time zone from the *Set Time Zone* drop down list.
- 5 Enter the interval, in hours, at which to want the Router to resynchronize with the SNTP Server, at the *Synchronization Interval* text box. The default is every 24 hours.
- 6 Select a primary SNTP server, and if required a secondary SNTP server from the appropriate drop down boxes.
- 7 If you want to enable daylight saving, check the *Daylight Savings* check box.
- 8 Select the month and day that you want daylight savings to begin at *Start Time*, and select the month and day that you want daylight savings to end at *End Time*.



The Daylight Savings option advances the system clock by one hour between the dates that you specify in the Start Time and End Time drop down lists. It does not cause the system clock to be updated for daylight savings time automatically.

- 9 Click *Apply* to save the settings.

Advanced

From the Advanced Screen, you can configure:

- NAT (Network Address Translation) and IPSec NAT-T (NAT Traversal) Pass-through
- Universal Plug and Play
- WAN Ping Blocking
- Remote Administration

The sub-menu topics in the Advanced menu also enable you to configure Routing options, and to configure Dynamic DNS.

- NAT**
- *NAT* — Before you disable this function, make sure you have changed the administrator password. Network Address Translation (NAT) is the method by which the router shares the single IP address assigned by your ISP with the computers on your network.

This function should only be disabled if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur.

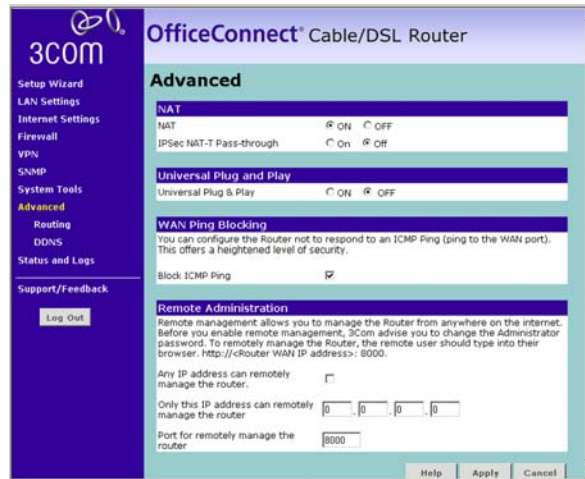
- *IPSec NAT-T Pass-through* — NAT-T (NAT Traversal) is an Internet Draft proposed to IETF in order to help the problems associated with passing IPSec traffic through NAT Routers. For NAT-T to work, both ends of the connection need to support this function.

Ensure that you enable *NAT-T* only if it is needed, as it will reduce LAN-WAN throughput. The OfficeConnect Cable/DSL Router supports NAT-T draft 2 implementation.

To configure NAT, and IPsec NAT-T Pass-through:

- 1 Select *Advanced* from the main menu. The *Advanced* screen displays (Figure 55).

Figure 55 Advanced



- 2 To disable NAT, select the *OFF* radio button.



3Com recommends that you leave NAT enabled for maximum security.

- 3 To enable IPsec NAT-T Pass-through, select the *On* radio button.
- 4 If required, continue configuring advanced options on this screen, or click *Apply* to save the settings.

Universal Plug and Play

Universal Plug and Play is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are Universal Plug and Play compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is Universal Plug and Play compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the Universal Plug and Play feature disabled. If you

want to use any applications that are Universal Plug and Play compliant, you can enable this feature. To enable Universal Plug and Play:

- 1 Select *Advanced* from the main menu. The *Advanced* screen displays [\(Figure 55\)](#).
- 2 To enable Universal Plug and Play, select the *ON* radio button.
- 3 If required, continue configuring advanced options on this screen, or click *Apply* to save the settings.

WAN Ping Blocking

Computer hackers use what is known as "Pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there.

The Router can be set up so it will not respond to an ICMP Ping from the outside. This heightens the level of security of your Router.

To turn off the ping response:

- 1 Select *Advanced* from the main menu. The *Advanced* screen displays [\(Figure 55\)](#).
- 2 Check the *Block ICMP Ping* check box.
- 3 If required, continue configuring advanced options on this screen, or click *Apply* to save the settings.

Remote Administration

Remote Administration allows you to make changes to your Router's settings from anywhere on the Internet. You can choose to either:

- Enable any PC on the network to remotely manage your Router
- Enter one specific IP address that can remotely manage your router. This is more secure, as only the specified IP address will be able to manage the Router



Before you enable this function, ensure that you have set the Administration Password.

To set up remote administration:

- 1 Select *Advanced* from the main menu. The *Advanced* screen displays [\(Figure 55\)](#).
- 2 Either:

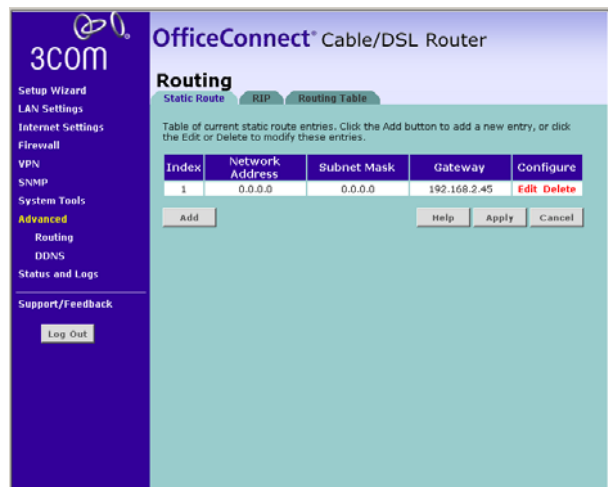
- Check the *Any IP address can remotely manage the router* check box if you want any PC to be able to remotely manage the Router. Or,
 - Enter the IP address of the PC that you want to remotely manage the Router in the *Only this IP address can remotely manage the router* check box
- 3 Enter the number of the port that will be used to remotely manage the Router in the *Port for remotely manage the router* text box. This must be entered in the browser as part of the URL when the remote user logs in.
 - 4 Click *Apply* to save the settings.

Routing This sub-menu option displays three tabs along the top of the main screen: *Static Route*, *RIP* and *Routing Table*.

Static Route

The Router supports static route functionality. Select the *Static Route* tab from the *Advanced > Routing* sub-menu to display the screen shown in [Figure 56](#)

Figure 56 Static Route screen



The following information is displayed for each static route:

- Index - the index of the static route
- Network Address - the network address of the route. If network address and subnet mask are both set to 0.0.0.0, this is the default route.

- Subnet Mask - the subnet mask of the route. If network address and subnet mask are both set to 0.0.0.0, this is the default route.
- Gateway - the gateway used to route data to the network specified by the network address.

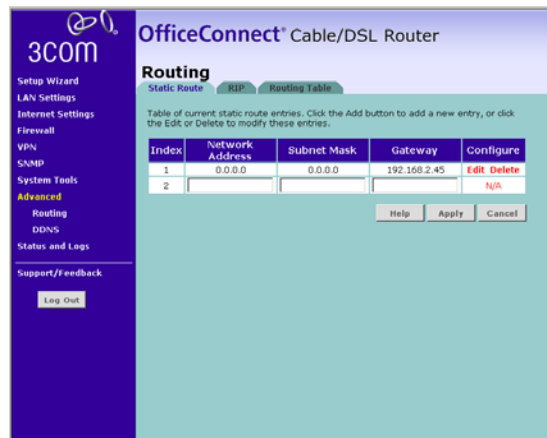
To configure a static route:

- 1 Click on *Add* to add a new route, or click *Edit* in the Configure column to edit an existing entry. The Add/Edit Static Route screen displays (Figure 57).



You can delete an existing entry by clicking on *delete* in the Configure column.

Figure 57 Add/Edit Static Route Screen



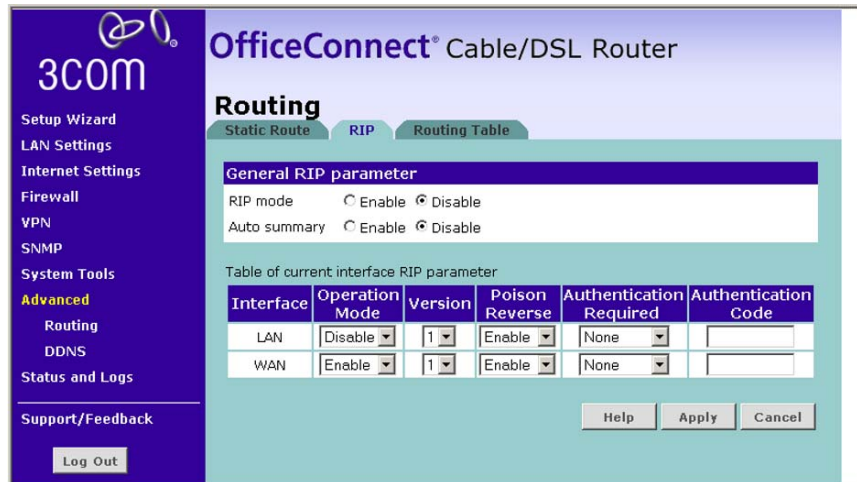
- 2 Enter the *Network Address*, *Subnet Mask* and *Gateway* for this route, and click *Apply*. The route is added to the Static Route table.

RIP

The Router supports the Routing Information Protocol (RIP). RIP allows you to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network. LAN and WAN interfaces can be configured independently of each other.

Select the *RIP* tab from the *Advanced > Routing* sub-menu to display the screen shown in [Figure 58](#)

Figure 58 RIP screen



To set up RIP and auto summary, and to set up or change information for the LAN interface, the WAN interface or both:

- 1 Check the *RIP Mode - Enable* check box to configure RIP on the Router.
- 2 Check the *Auto Summary - Enable* check box if you want the Router to send simplified routing data to other RIP devices, instead of full routing data.
- 3 Select one of *Disable*, *Enable* or *Silent* from the *Operation Mode* drop-down list. If you select *Enable*, the Router transmits RIP update information to other RIP enabled devices. If you select *Silent*, the Router only receives RIP update messages.
- 4 Select either *1* (for RIPv1) or *2* (for RIPv2) from the *Version* drop-down list. 3Com recommends that you use RIPv1 if there is any RIP enabled device on your network that does not support RIPv2. In all other case, select RIPv2.
- 5 Select either *Enable* or *Disable* from the *Poison Reverse* drop-down list. Enabling *Poison Reverse* on your Router allows it to indicate to other RIP-enabled devices that they both have routes that point to each other, preventing data loops.
- 6 Select either *None* or *Password* from the *Authentication Required* drop-down list. If you select *Password*, an unencrypted text password must be set on all RIP-enabled devices.
- 7 If you selected *Password* at step 6, enter a password at the *Authentication Code* prompt.

- 8 Click *Apply* to save the settings.

Routing Table

Select the *Routing Table* tab from the *Advanced > Routing* sub-menu to display routing information used by the Router. The information is displayed in the format shown in [Figure 59](#)

Figure 59 Routing Table screen

3COM OfficeConnect® Cable/DSL Router

Routing

Static Route RIP Routing Table

Flags	Network Address	Netmask	Gateway	Interface	Metric
C	192.168.1.0	255.255.255.0	directly	LAN	0
C	127.0.0.1	255.255.255.255	directly	Loopback	0

Flags : C - directly connected, S - static, R - RIP, I - ICMP Redirect

Help

Log Out

DDNS Dynamic Domain Name Server (DDNS) enables you to map a static domain name to a dynamic IP address. The Router supports two DDNS providers, TZO.com and DYNDNS. Before you can set up DDNS, you must obtain an account, password and static domain name from your DDNS provider. DDNS is disabled by default.

To set up DDNS:

- 1 Select *Advanced* from the main menu, then select *DDNS* from the sub-menu. The DDNS screen displays (Figure 60).

Figure 60 DDNS screen

The screenshot shows the 'OfficeConnect® Cable/DSL Router' interface. On the left is a navigation menu with 'Advanced' highlighted. The main area is titled 'Dynamic Domain Name Server (DDNS)'. Below the title is a descriptive paragraph: 'DDNS allows users to map a static Domain Name to a dynamic IP address. However, You must get an account, password, and your static Domain Name from a DDNS service provider. This router supports DDNS services from www.dyndns.org and www.tzo.com.' Below this is a 'DDNS Configuration' section with a 'Dynamic DNS' header and two radio buttons: 'Enable' (selected) and 'Disable'. There are four input fields: 'Provider' (a dropdown menu showing 'TZO.com'), 'Domain Name' (with 'DynDNS.org' and 'TZO.com' as suggestions), 'E-mail', and 'Key'. At the bottom right are 'Help', 'Apply', and 'Cancel' buttons.

- 2 Select the *Dynamic DNS Enable* radio button.
- 3 Select a DDNS Service *Provider* from the drop-down list. This can be either TZO.com or DynDNS.

TZO.com

If you select TZO.com:

- 1 In the *Domain Name* text box, enter the domain name.
- 2 In the *E-mail* text box, enter the account name.
- 3 In the *Key* text box, enter the account password.
- 4 Click *Apply* to make this service active.

DynDNS

If you select DYNDNS:

- 1 In the *Domain Name* text box, enter the domain name.
- 2 In the *Account* text box, enter the account name.
- 3 In the *Password* text box, enter the account password.
- 4 Click *Apply* to make this service active.

Status and Logs

Selecting *Status and Logs* from the main menu displays the Status Screen, and also displays two sub-menus: *Traffic Metering* and *Logs*.

Status You can use the Status Screen to view general information about your Router, including the version numbers of your router's software and hardware. You can also check the status of Internet connections, Internet settings and LAN settings.

To view the Status screen:

- 1 Select *Status and Logs* from the main menu. The screen shown in [Figure 61](#) displays:

Figure 61 Status Screen



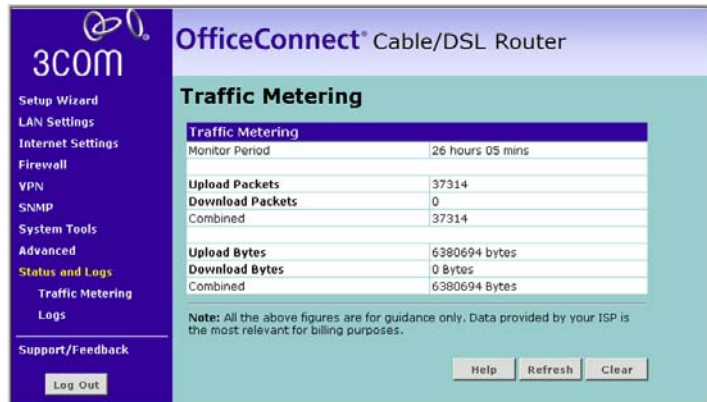
- 2 If required, click *Renew* to update the displayed information, or click *Release* to ...

Traffic Metering The Traffic Metering screen displays the amount of data transmitted to and received from the Internet. This information is provided for guidance only, and may differ from that used by your ISP for billing purposes.

To view the Traffic Metering screen:

- 1 Select *Status and Logs* from the main menu, then select the *Traffic Metering* sub-menu. The screen shown in [Figure 62](#) displays:

Figure 62 Traffic Metering Screen



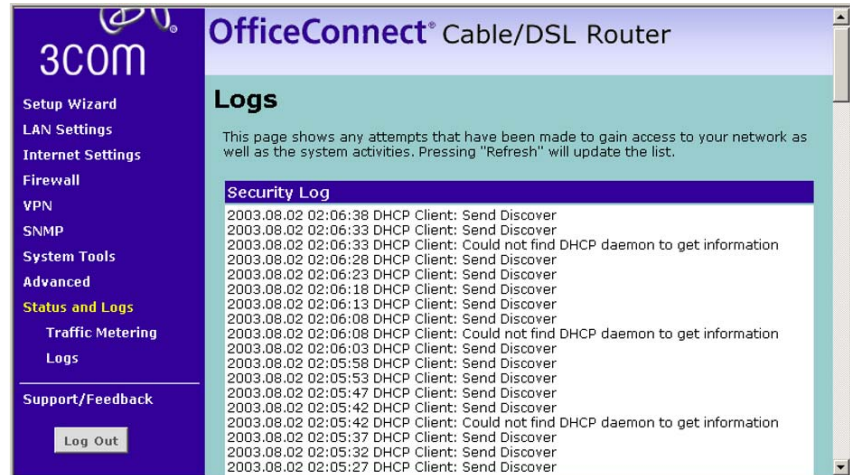
- 2 If required, click *Refresh* to update the displayed information.

Logs The Logs screen shows any attempts that have been made to gain access to your network, as well as the system activities.

To display log information:

- 1 Select *Status and Logs* from the main menu, then select *Logs* from the sub-menu. The Logs screen displays (Figure 63):

Figure 63 Logs Screen



- 2 Either:
 - Click *Refresh* to update the display. Or,
 - Click *Clear* to clear the log (note that all current entries will be erased). Or,
 - Click *Save* to save the log to disk in a text file. When prompted for a location to save the file to, specify a filename and location, and then click *OK*.

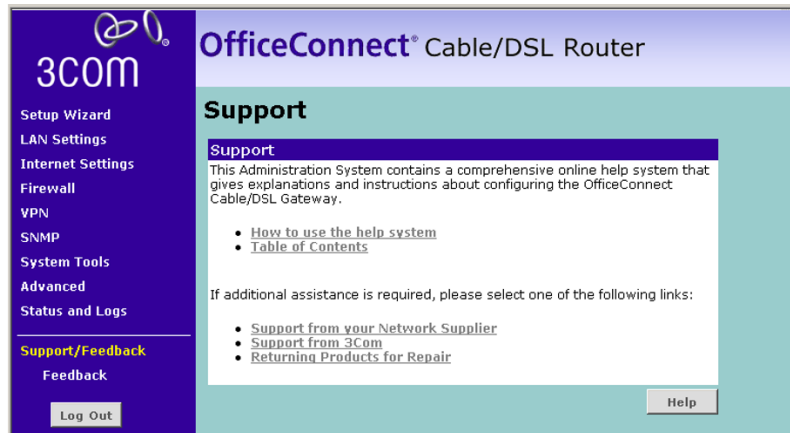
Support/Feedback

Selecting *Support/Feedback* from the main menu displays the *Support* screen and the *Feedback* sub-menu topic.

Support

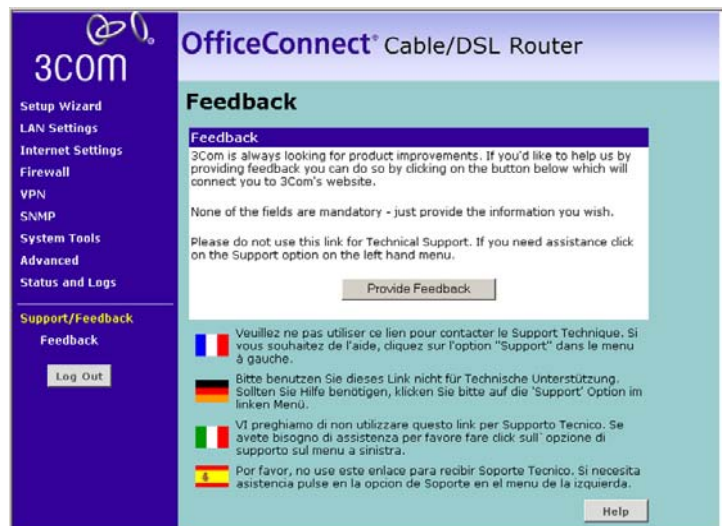
Selecting the *Support* option on the main menu displays the support links screen, which contains a list of Internet links that provide information and support concerning the Router (Figure 64).

Figure 64 Support Screen



Feedback Selecting the *Feedback* option on the sub-menu displays the Feedback screen and allows you to provide feedback to 3Com on the operation of your Router (Figure 65). This screen should not be used to obtain technical support.

Figure 65 Feedback Screen



6

TROUBLESHOOTING

Basic Connection Checks

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the LAN Status LED and Cable/DSL Status LED on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the LAN Status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Router Configuration Screens

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Router and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in [Chapter 3, Setting Up Your Computers](#). Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.
- When entering the address of the Router into your web browser, ensure that you use the full URL including the http:// prefix (for example, **http://192.168.1.1**).
- Ensure that you do not have a Web proxy enabled on your computer. Go to the *Control Panel* and click on *Internet Options*. Select the

Connections tab and click on the *LAN Settings* button at the bottom. Make sure that the *Proxy Server* option is unchecked.

- If you cannot browse to the Router, use the *winiipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Router.

From the *Start* menu, choose *Run* and then enter **winiipcfg**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router address is 192.168.1.1. If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Router.

Under Windows 2000 and Windows XP, use the *ipconfig* command-line utility to perform the same functions.

Connecting to the Internet

If you can browse to the Router configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the cable/DSL modem is OK, and that the Cable/DSL Status LEDs on both Router and modem are illuminated.
- Confirm that the connection between the modem and the cable/DSL interface is OK.
- Ensure that you have entered the correct information into the Router configuration screens as required by your Internet Service Provider. Use the “Internet Settings” screen to verify this. Refer to [“Internet Settings”](#) on [page 42](#).
- For DSL users, check that the PPPoE or PPTP user name, password and service name are correct, if these are required. Only enter a PPPoE service name if your ISP requires one.
- For cable users, check whether your ISP requires a fixed MAC (Ethernet) address or Host Name. If so, use the Hostname and MAC Address screen in Internet settings to ensure that the correct Host Name or MAC address is presented. Refer to [“Hostname & MAC”](#) on [page 50](#).
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel > Internet Options > Connections*.

Forgotten Password and Reset to Factory Defaults

If you can browse to the Router configuration screen but cannot log in because you do not know or have forgotten the password, follow the steps below to reset the Router to its factory default configuration.



CAUTION: *All your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when the reset would be convenient.*

- 1 Remove power from the Router.
- 2 Disconnect all your computers and the cable/DSL modem from the Router.
- 3 Using a straight through Ethernet cable, connect the Ethernet Cable/DSL port on the rear of the Router to any one of the LAN ports.
- 4 Re-apply power to the Router. The Alert LED will flash as the Router starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly, remove power from the Router.
- 5 Remove the cable connecting the Cable/DSL port to the LAN port, and reconnect one of your computers to one of the Router LAN ports.
- 6 Re-apply power to the Router, and when the start-up sequence has completed, browse to:

http://192.168.1.1

and run the Setup Wizard. You may need to restart your computer before you attempt this.

- 7 When the Setup Wizard has completed, you may reconnect your network as it was before.

Alert LED

The Alert LED will flash when the Router unit is first powered up while the system software checks the hardware for proper operation. Once the Router has started normal operation, the Alert LED will go out.

- If the Alert LED does not go out following start up, but illuminates continuously, this indicates that the software has detected a possible fault with the hardware. Remove power from the Router, wait 10 seconds and then re-apply power. If the Alert LED comes on continuously again, then a fault has been detected. Locate the copy of

the Router software on the accompanying CD-ROM or 3Com web site (<http://www.3com.com>) and upload it to the Router to see if this clears the fault (refer to “Recovering from Corrupted Software” below). If this does not fix the problem, contact your supplier for further advice.

- During normal operation, you may notice the Alert LED lighting briefly from time to time. This indicates that the Router has detected a hacker attack from the Internet and has prevented it from harming your network. You need take no specific action on this, unless you decide that these attacks are happening frequently in which case you may wish to discuss this with your ISP. The Router logs such attacks, and this information is available through the Status and Logs screens.

Power LED or Power Adapter OK LED Not Lit

- Check that your Router is receiving power by looking at the status of the Power LED on the front panel and the Power Adapter OK LED on the rear panel:
 - If both LEDs are lit green then the unit is receiving power.
 - If both LEDs are unlit then no power is being supplied to the unit. Check that the power adapter is plugged into a working mains outlet and that the mains outlet is supplying power. If the mains socket is supplying power then the power adapter or power adapter connection may be faulty. See [“Replacement Power Adapters”](#) below.
 - If the Power Adapter OK LED is lit but the Power LED is unlit then there may be a fault with your unit. Contact 3Com Technical Support.
- Check that you are using the correct power adapter for your Router. You should only use the power adapter supplied with your Router.

Replacement Power Adapters

If both the Power Adapter OK LED and Power LED are off, check your power adapter connection. If the mains outlet is working and is capable of supplying power to other devices, contact 3Com Technical Support and ask for a replacement power adapter. Please quote the power adapter part number shown on the OfficeConnect power adapter you are using.

Alternatively, quote the part number for your region:

Table 3 Power Adapter Part Numbers

Part Number	Region
3C16760	US and Canada
3C16761	UK
3C16762	Europe and Middle East
3C16763	Australasia (except Japan and Korea)
3C16764	South Africa
3C16766	Japan
3C16767	Korea
3C16768	Argentina

Recovering from Corrupted Software

If the system software has become corrupted, the Router will enter a “recovery” state; DHCP is enabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Router unit in this state.

Before you start, ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.



The latest software is available on 3Com's Web site at:

www.3com.com

- 1** Remove power from the Router and disconnect all your computers, except for the one computer with the software image.
- 2** Reconfigure this computer to obtain an IP address automatically (see [“Obtaining an IP Address Automatically”](#) on [page 21](#))
- 3** Restart the computer, and re-apply power to the Router.
- 4** Using the Web browser on the computer, enter the following URL in the location bar:
`http://192.168.1.1.`
This will connect you to the Recovery utility in the Router.
- 5** Follow the on-screen instructions. Enter the path and filename of the software image file.
- 6** When the upload has completed, the Router will restart, run the self-test and, if successful, resume normal operation.

- 7 Refer to the Installation Guide to reconnect your Router to the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Router does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

Frequently Asked Questions

How do I reset the Router to Factory Defaults?

Either:

- If you can log in, refer to [“Reset to Factory Defaults”](#) on [page 73](#). Or
- If you have forgotten your password, and can not log on, see [“Forgotten Password and Reset to Factory Defaults”](#) on [page 93](#).

How many computers on the LAN does the Router support?

A maximum of 253 computers on the LAN are supported.

There are only 4 LAN ports on the Router. How are additional computers connected?

You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. 3Com wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

<http://www.3com.com/>

Does the Router support virtual private networks (VPNs)?

The Router has a Virtual Private Network (VPN) feature that provides a secure link between remote users and the corporate network by establishing an authenticated and encrypted tunnel for passing secure data over the Internet. Refer to [“VPN”](#) on [page 64](#).

Where can I download software updates for the Router?

Updates to the Router software are posted on the 3Com support web site, accessible by visiting:

<http://www.3com.com>

After you have downloaded the software from the 3Com Web site, you can upgrade your Router as described in ["Upgrade"](#) on [page 75](#).

A

IP ADDRESSING

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

Managing the Router over the Network

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.



The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is '192.168.100.8'. However, the size of the network determines the structure of this IP Address. In using the Router, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of '192.168.100.8' is split into two parts:

- Part one ('192.168.100') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.255.0'.

See [Table 4](#) for an example about how a network with three computers and a Router might be configured.

Table 4 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Router	192.168.100.72	255.255.255.0

Type Two

In larger networks, where there are more devices, the IP address of '192.168.100.8' is, again, split into two parts but is structured differently:

- Part one ('192.168') identifies the network on which the device resides.
- Part two ('.100.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.0.0'.

See [Table 5](#) for an example about how a network (only four computers represented) and a Router might be configured.

Table 5 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Router	192.168.002.72	255.255.0.0

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows® 95, Windows 98 or Windows NT 4.0. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves

an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000.

B

ISP INFORMATION

Information Regarding Popular ISPs

WAN Types	Characteristics	Popular ISPs
Dynamic IP (Clone MAC)	Cable modem ISP, non-hostname based. Need to clone the MAC address in the Advanced tab of the Internet Settings page.	MediaOne, RoadRunner, Optimum Online, Time Warner, Charter, Adelphia, Metrocast.
Dynamic IP (Hostname)	Cable ISP, Requires Hostname to authenticate ie. cx213818-B. Need to enter the hostname in the Internet Settings page.	@Home Network, Cogoco, ComCast, Cox, Excite, Rogers, Shaw, Insight, Videotron
PPPoE (DSL)	Usually special software installed on PC, MacPOET/WinPOET, EnterNet 300. The Router has this software built in and you can remove it from your PC. You will need to enter the user name and password that your ISP provided to you in the PPPoE page of the Router. Leave the service name blank unless your ISP requires it.	Bell*, Century Tel, Citizens, Primus, Prodigy, Snet, Sprint FC, Verizon, First World, Brightnet, Earthlink, Ameritech, Covad, Mindspring, Sympatico DSL, USwest, Owest, SNet
PPTP	Cable or DSL, always on. Some European ISPs require a PPTP tunnel to authenticate their network.	KPN (Netherlands), Austria Telecom

Static (DSL)	DSL Modem, always on. Need to enter ALL IP information from ISP in the Static IP address section of the Internet Settings page.	CableSpeed, Cnet, Direct Link, Drizzle, DSL Extreme, Earthlink Wireless, Fast Point, Flashcom, GTE-WhirlWind, Heavenet, HSA Corp, I-55, InterAccess, LinkLine, Mission, Naticom, NAS, Omitel, Onterra, Phatpipe, Rhythms, Speakeasy, Sterling, XO, Zyan
Static (Cable)	Cable Modem, Always on, ISP assigns specific IP information which needs to be entered on the "Fixed IP" page of the Router.	Cox Cable, Sprint, US Cable, Cable-Cable

*Bell includes Bell Advantage, Bell Canada, Bell South, PacBell and Southwestern Bell.

C

TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the OfficeConnect Cable/DSL Router.

OfficeConnect Cable/DSL Router

Interfaces

Cable/DSL modem connection — 10 Mbps/100 Mbps dual speed Ethernet port (10BASE-T/100BASE-TX)

LAN connection — four 10Mbps/100Mbps dual speed Ethernet ports (10BASE-T/100BASE-TX)

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

7VA, 23.9 BThU/hr

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

- Width = 220 mm (8.7 in.)
- Depth = 135.4 mm (5.2 in.)
- Height = 24.2 mm (1 in.)

Weight

535 g (1.3 lb)

Standards Functional: ISO 8802/3
IEEE 802.3

Safety: UL60950
 EN 60950
 CSA 22.2 #60950
 IEC 60950

EMC: EN 55022 Class B
 EN 55024
 CISPR 22
 FCC Part 15 Class B*
 ICES-003 Class B
 CNS 13438 Class A
 ETSI EN 301 489–17

Environmental: EN 60068 (IEC 68)

*See [“Regulatory Notices”](#) on [page 129](#) for conditions of operation.

System Requirements Operating Systems

The Router will support the following Operating Systems:

- Windows 95/98
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Mac OS 8.5 or higher
- Unix

Ethernet Performance The Router complies to the IEEE 802.3i, u and x specifications.

Cable Specifications The Router supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).

D

SAFETY INFORMATION

Important Safety Information



WARNING: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully. You must read the following safety information carefully before you install or remove the unit:



WARNING: Exceptional care must be taken during installation and removal of the unit.



WARNING: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.



WARNING: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.



WARNING: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.



WARNING: There are no user-replaceable fuses or user-serviceable parts inside the Router. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.



WARNING: Disconnect the power adapter before moving the unit.



WARNING: RJ-45 ports. These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.

Wichtige Sicherheitshinweise



VORSICHT: Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.

Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen:



VORSICHT: Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.



VORSICHT: Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.



VORSICHT: Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.



VORSICHT: Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.



VORSICHT: Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Router haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.



VORSICHT: Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.



VORSICHT: RJ-45-Anschlüsse. Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.

Consignes importantes de sécurité



AVERTISSEMENT: Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes. Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:



AVERTISSEMENT: Faites très attention lors de l'installation et de la dépose du groupe.



AVERTISSEMENT: Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.



AVERTISSEMENT: La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.



AVERTISSEMENT: L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.



AVERTISSEMENT: Il n'y a pas de parties remplaçables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.



AVERTISSEMENT: Débranchez l'adaptateur électrique avant de retirer cet appareil.



AVERTISSEMENT: Ports RJ-45. Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.

Información de seguridad importante



ADVERTENCIA: Las advertencias contienen indicaciones que debe respetar por su seguridad personal. Siga las indicaciones con cuidado.



Antes de instalar o retirar la unidad, debe leer detenidamente la siguiente información de seguridad.



ADVERTENCIA: Debe tener especial cuidado durante la instalación y retirada de la unidad.



ADVERTENCIA: Para garantizar el cumplimiento de las normas internacionales de seguridad, utilice únicamente el adaptador de corriente suministrado con la unidad.



ADVERTENCIA: El enchufe debe estar cerca de la unidad y ser de fácil acceso. La única forma de cortar la alimentación de la unidad consiste en desconectar el cable eléctrico de la toma de corriente.



ADVERTENCIA: Esta unidad funciona en condiciones SELV (voltaje extrabajo de seguridad) de conformidad con la norma IEC 950. Las condiciones sólo se mantienen si el equipo al que esté conectada la unidad también funciona en condiciones SELV.



ADVERTENCIA: La unidad no contiene fusibles ni piezas que el usuario pueda sustituir o reparar. Si tiene un problema físico con la unidad que no se pueda resolver mediante las acciones de solución de problemas de esta guía, póngase en contacto con su proveedor.



ADVERTENCIA: Desconecte el adaptador de corriente antes de mover la unidad.



ADVERTENCIA: Puertos RJ-45. Son conectores de datos RJ-45 blindados. No pueden utilizarse como tomas de teléfono tradicionales estándar ni para conectar la unidad a una central de conmutación PBX tradicional ni a una red telefónica pública. Conecte sólo conectores de datos RJ-45, sistemas de telefonía de red local o teléfonos de red local a estas tomas.



Pueden conectarse cables de datos blindados o sin blindar con clavijas blindadas o sin blindar a estos conectores de datos.

E

OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at <http://eSupport.3com.com/>. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request.

Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com Extended Warranty and Professional Services is available at <http://www.3com.com/>

Contact your authorized 3Com reseller or 3Com for additional product and support information.

Troubleshoot Online

You will find support tools posted on the 3Com web site at <http://www.3com.com/>

- **3Com Knowledgebase** helps you troubleshoot 3Com products. This query-based interactive tool is located at <http://knowledgebase.3com.com> and contains thousands of technical solutions written by 3Com support engineers.
- **Connection Assistant** helps you install, configure and troubleshoot 3Com desktop and server NICs, wireless cards and Bluetooth devices. This diagnostic software is located at:

http://www.3com.com/prodforms/software/connection_assistant/ca_thankyou.html

Access Software Downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at <http://eSupport.3com.com/>.

First time users will need to apply for a user name and password. A link to software downloads can be found at <http://eSupport.3com.com/>, or under the Product Support heading at <http://www.3com.com/>

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below. You will find a current directory of support telephone numbers posted on the 3Com web site at <http://csoweb4.3com.com/contactus/>

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at <http://eSupport.3com.com/>

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will

be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at <http://eSupport.3com.com/>. First time users will need to apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of support telephone numbers posted on the 3Com web site at <http://csoweb4.3com.com/contactus/>

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair			
Australia	1 800 678 515	Philippines	1235 61 266 2602 or
Hong Kong	800 933 486		1800 1 888 9469
India	+61 2 9424 5179 or	P.R. of China	800 810 3033
	000800 650 1111	Singapore	800 6161 463
Indonesia	001 803 61009	S. Korea	080 333 3308
Japan	00531 616 439 or	Taiwan	00801 611 261
	03 3507 5984	Thailand	001 800 611 2000
Malaysia	1800 801 777		
New Zealand	0800 446 398		
Pakistan	+61 2 9937 5083		
You can also obtain support in this region using the following e-mail: apr_technical_support@3com.com			
Or request a repair authorization number (RMA) by fax using this number:			+ 65 543 6348

Europe, Middle East, and Africa Telephone Technical Support and Repair

From anywhere in these regions, call: +44 (0)1442 435529

From the following countries, you may use the numbers shown:

Austria	01 7956 7124	Luxembourg	342 0808128
Belgium	070 700 770	Netherlands	0900 777 7737
Denmark	7010 7289	Norway	815 33 047
Finland	01080 2783	Poland	00800 441 1357
France	0825 809 622	Portugal	707 200 123
Germany	01805 404 747	South Africa	0800 995 014
Hungary	06800 12813	Spain	9 021 60455
Ireland	1407 3387	Sweden	07711 14453
Israel	1800 945 3794	Switzerland	08488 50112
Italy	199 161346	U.K.	0870 909 3266

You can also obtain support in this region using the following URL:

<http://emea.3com.com/support/email.html>

Country	Telephone Number	Country	Telephone Number
Latin America Telephone Technical Support and Repair			
Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region using the following:

Spanish speakers, enter the URL:

<http://lat.3com.com/lat/support/form.html>

Portuguese speakers, enter the URL:

<http://lat.3com.com/br/support/form.html>

English speakers in Latin America should send e-mail to:

lat_support_anc@3com.com

US and Canada Telephone Technical Support and Repair

1 800 876 3266

F

END USER SOFTWARE LICENSE AGREEMENT

IMPORTANT: READ BEFORE INSTALLING THE SOFTWARE
3Com END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE: 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING: You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union (EU) resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT: This product, Software and/or technical data (collectively "Product") may contain encryption. This Product is subject to U.S. and EU export control laws and regulations and may be subject to export or import regulations in other countries, including controls on encryption products. You agree that you will not export, reexport or transfer the Product (or any copies thereof) or any products utilizing the Product in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, reexport, transfer or import the Product.

In addition to the above, the Product may not be used by, or exported or reexported to (i) any U.S.- or EU- sanctioned or embargoed country, or to nationals or residents of such countries; or (ii) to any person, entity, organization or other party identified on the U.S. Department of Commerce's Table of Denial Orders or the U.S. Department of Treasury's lists of "Specially Designated Nationals and Blocked Persons," as published and revised from time to time; (iii) to any party engaged in nuclear, chemical/biological weapons or missile proliferation activities, unless authorized by U.S. and local (as required) law or regulations.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of

3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as iCommercial Computer Software[®] as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

GOVERNING LAW: This Agreement shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write: 3Com Corporation, Customer Support Information, 350 Campus Drive, Marlborough, MA 01752-3064

3Com Corporation

350 Campus Drive,

Marlborough, MA 01752-3064

Copyright © 2004 3Com Corporation and its licensors. All rights reserved. 3Com is a registered trademark of 3Com Corporation.

GLOSSARY

- 10BASE-T** The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.
- 100BASE-TX** The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
- Access Point** An Access Point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.
- Auto-negotiation** Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.
- Bandwidth** The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.
- Category 3 Cables** One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

Category 5 Cables One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Client The term used to describe the desktop PC that is connected to your network.

DHCP Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DDNS Dynamic Domain Name Server. A method that enables Internet users to tie their domain name(s) to computers or servers. DDNS enables a domain name to follow an IP address automatically when the IP address changes.

DNS Server Address DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL modem DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

Encryption A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.

- Ethernet** A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.
- Ethernet Address** See MAC address.
- Fast Ethernet** An Ethernet system that is designed to operate at 100 Mbps.
- Firewall** Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.
- Full Duplex** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
- Half Duplex** A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.
- Hub** A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.
- IEEE** Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.
- IETF** Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.
- Infrastructure mode** Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)
- IP** Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address

consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

IP Address Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

ISP Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

MAC Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address Media Access Control Address. Also called the hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

NAT Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC)	A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.
Protocol	A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.
PPPoE	Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.
PPTP	Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the internet.
RIP	Routing Information Protocol. RIP allows an administrator to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.
RJ-45	A standard connector used to connect Ethernet networks. The "RJ" stands for "registered jack".
Router	A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.
Server	A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.
SPI	Stateful Packet Inspection. This feature requires the firewall to remember what outgoing requests have been sent and only allow responses to those requests back through the firewall. This way, un-requested attempts to access the network will be denied.
SSID	Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.
Subnet Address	An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

- Subnet mask** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).
- Subnets** A network that is a component of a larger network.
- Switch** A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.
- TCP/IP** Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.
- TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.
- Traffic** The movement of data packets on a network.
- universal plug and play** Universal plug and play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.
- URL Filter** A URL Filter is a feature of a firewall that allows it to stop its clients from browsing inappropriate Web sites.
- VPN** Virtual Private Network. A VPN is a private network where the data is passed across a public network infrastructure such as the Internet. The data is kept private by using encryption.

- WAN** Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.
- WEP** Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.
- Wizard** A Windows application that automates a procedure such as installation or configuration.

INDEX

A

access control 57
 Addresses
 IP 99
 admin password
 resetting 76
 administration
 remote 81
 Advanced
 RIP 83
 routing table 85
 Automatic Addressing 101

B

backup settings 74

C

Cable Specifications 106
 client IP filters 57
 access control 57
 schedule rule 60
 URL filter 59
 Connection Policy 53
 Conventions
 notice icons, About This Guide 8
 text, About This Guide 8

D

DDNS 86
 DHCP 37, 101
 DHCP Server 23
 DMZ 63
 DNS 22, 49
 DoS attacks 51
 DOS detect criteria
 configuring 54
 Dynamic IP Address 30, 42

F

factory defaults
 reset to 73
 feedback 90
 Firewall
 client IP filters 57
 DMZ 63
 Intrusion Detection 52
 MAC address filtering 62
 special applications 54
 SPI 51
 virtual servers 56
 Forgotten Password 93

H

Hostname
 configuring 50

I

Internet
 addresses 99
 Internet Addressing Mode 29
 Internet Settings
 dynamic IP address 42
 PPPoE 42
 PPTP 43
 static IP address 43
 Intrusion Detection 52
 IP Address 34, 37, 48, 99

L

L2TP 43, 47
 LED 14
 logs 88

M

MAC Address 30, 36, 44, 50
 configuring 50
 MAC address filtering 62

N

NAT 79
 Network
 addresses 99

P

ping blocking 81
plug and play 80
PPPoE 24, 31, 42
PPTP 43

R

remote administration 81
Reset to Factory Defaults 93
reset to factory defaults 73
restart router 73
restore settings 74
RIP 83
routing 82
 RIP 83
 routing table 85
 static route 82
routing table 85

S

Safety Information 17
schedule rule 60
Setup Wizard 25
SNMP 71
special applications 54
Specifications
 technical 105
SPI 51
Static Addressing 101
Static IP Address 43
static route 82
status 86
Subnet Mask 34, 37, 48, 99
Summary 38
support 89
Support Links 89
System Tools 72

T

TCP/IP 21, 23, 37, 99
technical
 specifications 105
 standards 105
Time Zone 27
time zone
 configuring 77
traffic metering 88

U

universal plug and play 80
upgrade 75
URL filter 59

V

virtual servers 56

W

WAN 29
WAN ping blocking 81
Web Proxy 24

REGULATORY NOTICES

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

FCC DECLARATION OF CONFORMITY

We declare under our sole responsibility that the

Model: 3CR858-91 **Description:** Cable/DSL Router

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement
- Federal Communications Commission 47 CFR Part 15, subpart B
 - 15.107 (a) Class B Conducted Limits
 - 15.109 (a) Class B Radiated Emissions Limits
- 15.107 (e) Class B Conducted Limits
- 15.109 (g) Class B Radiated Emissions Limits

CSA STATEMENT

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

CE STATEMENT (EUROPE)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

VCCI STATEMENT

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

FCC



CAUTION: To assure continued compliance, (for example, use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment

3Com Corporation, Corporate Headquarters,
350 Campus Drive, Marlborough, MA
USA 01752-3064

To learn more about 3Com products and services,
visit our World Wide Web site at www.3com.com

All specifications are subject to change without notice.

Copyright © 2004 3Com Corporation. All rights reserved.
3Com and are registered trademarks of 3Com
Corporation. All other company and product names may
be trademarks of their respective companies.

DUA8589-1AAA01
Rev. 01

